Extreme Networks EAS 100-24t Switch Software Manual

Layer 2 Managed Gigabit Switch

Release 1.00

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
(408) 579-2800
http://www.extremenetworks.com

Published: July 2011
Part number: 120707-00 Rev. 01

AccessAdapt, Alpine, Altitude, BlackDiamond, Direct Attach, EPICenter, ExtremeWorks Essentials, Ethernet Everywhere, Extreme Enabled, Extreme Ethernet Everywhere, Extreme Networks, Extreme Standby Router Protocol, Extreme Turbodrive, Extreme Velocity, ExtremeWare, ExtremeWorks, ExtremeXOS, Go Purple Extreme Solution, ExtremeXOS ScreenPlay, ReachNXT, Ridgeline, Sentriant, ServiceWatch, Summit, SummitStack, Triumph, Unified Access Architecture, Unified Access RF Manager, UniStack, XNV, the Extreme Networks logo, the Alpine logo, the BlackDiamond logo, the Extreme Turbodrive logo, the Summit logos, and the Powered by ExtremeXOS logo are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and/or other countries.

sFlow is the property of InMon Corporation.

Specifications are subject to change without notice.

All other registered trademarks, trademarks, and service marks are property of their respective owners.

© 2011 Extreme Networks, Inc. All Rights Reserved.

Table of Contents

Preface Template Formats 7

Intended Readers 7
Typographical Conventions 7
Notes, Cautions, and Warnings 8

Chapter 1: Web-based (GUI) Configuration 9

Introduction 9
Login to Web Manager 9
Web-based User Interface 10
Areas of the User Interface 10
Web Pages 11

Chapter 2: Configuration 15

Device Information 15
System Information 16
Serial Port Settings 16
IP Address Settings 17
IPv6 Address Settings 19
IPv6 Route Settings 20
IPv6 Neighbor Settings 20
Port Configuration Folder 21
Port Settings 21
Port Description Settings 23
Port Error Disabled 25
Port Media Type 25
Static ARP Settings 26
User Accounts 27
System Log Configuration Folder 28
System Log Settings 28
System Log Server 28
DHCP Relay Folder 30
DHCP Relay Global Settings 30
DHCP Relay Interface Settings 31
MAC Address Aging Time 32
Web Settings 32
Telnet Settings 33
CLI Paging Settings 33
Firmware Information 34
SNTP Settings Folder 34
Time Settings 35
Time Zone Settings 35
SMTP Settings Folder 37
SMTP Service Settings 37
SMTP Service 38
SNMP Settings Folder 38
SNMP View Table 39
SNMP Group Table 40

SNMP User Table 42
SNMP Community Table 43
SNMP Host Table 44
SNMP Engine ID 44
SNMP Trap Configuration 45
RMON 45

Chapter 3: Layer 2 Features 47

Jumbo Frame 47
VLANs 47
802.1Q Static VLAN 54
Q-in-Q Folder 57
Q-in-Q Settings 58
VLAN Translation Settings 59
802.1v Protocol VLAN Folder 59
802.1v Protocol Group Settings 60
802.1v Protocol VLAN Settings 60
GVRP Settings 62
Asymmetric VLAN Settings 63
MAC-based VLAN Settings 63
PVID Auto Assign Settings 64
Port Trunking 65
LACP Port Settings 67
Traffic Segmentation 68
IGMP Snooping Folder 69
IGMP Snooping Settings 69
MLD Snooping Settings 71
MLD Control Messages 71
Port Mirror 74
Loopback Detection Settings Page 75
Spanning Tree Folder 76
STP Bridge Global Settings 79
STP Port Settings 80
MST Configuration Identification 82
STP Instance Settings 83
MSTP Port Information 84
Forwarding & Filtering Folder 85
Unicast Forwarding Settings 85
Multicast Forwarding Settings 86
Multicast Filtering Mode 86
LLDP Folder 87
LLDP Global Settings 88
LLDP Port Settings 89
LLDP Basic TLVs Settings 90
LLDP Dot1 TLVs Settings 90
LLDP Dot3 TLVs Settings 91

Chapter 4: Quality of Service (QoS) 93

Bandwidth Control 95
Traffic Control 95
802.1p Default Priority 98
802.1p User Priority 99
QoS Scheduling Settings 99
Priority Mapping 100
TOS Mapping 101

DSCP Mapping....102

Chapter 5: Security....103

Trusted Host....103
Port Security Folder....104
Port Security Port Settings....104
Port Security FDB Entries....105
Authentication Settings....105
802.1X Folder....106
802.1X Settings....110
802.1X User....111
Authentication RADIUS Server....112
SSL Settings....115
SSH Folder....117
SSH Settings....118
SSH Authmode and Algorithm Settings....118
SSH User Authentication Lists....120
Access Authentication Control Folder....121
Authentication Policy Settings....122
Application Authentication Settings....123
Authentication Server Group....124
Authentication Server....125
Login Method Lists....127
Enable Method Lists....128
Local Enable Password Settings....129
MAC-based Access Control Folder....130
MAC-based Access Control Settings....130
MAC-based Access Control Local Settings....132

Chapter 6: Access Control List (ACL)....135

ACL Configuration Wizard....135
Access Profile List....136
Access Profile List – Enternet ACL....137
Access Profile List – IPv4 ACL....142
Access Profile List – IPv6 ACL....147
Access Profile List – Packet Content ACL....152
ACL Finder....155
ACL Flow Meter....156

Chapter 7: Monitoring....159

Cable Diagnostics....159
CPU Utilization....159
Port Utilization....161
Packet Size....161
Memory Utilization....163
Packets Folder....164
Received (Rx)....164
UMB_cast (Rx)....166
Transmitted (Tx)....168
Errors Folder....170
Received (RX)....170
Transmitted (TX)....172
Port Access Control Folder....174
RADIUS Authentication....174
RADIUS Account Client....175

Authenticator State....176
Authenticator Statistics....178
Authenticator Session Statistics....181
Authenticator Diagnostics....183
Browse ARP Table....185
Browse VLAN....186
IGMP Snooping Folder....186
Browse IGMP Router Port....187
IGMP Snooping Group....187
IGMP Snooping Host....188
MLD Snooping Folder....188
Browse MLD Router Port....188
MLD Snooping Group....189
LLDP Folder....189
LLDP Statistics System....190
LLDP Local Port Information....190
LLDP Remote Port Information....191
MBA Authentication State....192
Browse Session Table....192
MAC Address Table....193
System Log....193

Chapter 8: Save and Tools....195

Save Configuration....195
Save Log....196
Save All....196
Configuration File Upload & Download....197
Upload Log File....197
Reset....198
Ping Test....198
Download Firmware....199
Reboot System....200

Appendix A: System Log Entries....201

Appendix B: Trap List....211

Preface Template Formats

This manual describes the software installation and configuration of the EAS 100-24t.

Intended Readers

The **Extreme Networks Software Installation Manual** contains information for setup and management of the Switch. This manual is intended for network managers familiar with network management concepts and terminology.

Typographical Conventions

Convention	Description
[ ]	In a command line, square brackets indicate an optional entry. For example: [copy filename] means that optionally you can type copy followed by the name of the file. Do not type the brackets.
Bold font	Indicates a button, a toolbar icon, menu, or menu item. For example: Click on the **Apply** button. Used for emphasis. May also indicate system messages or prompts appearing on screen. For example: **You have mail**. **Bold** font is also used to represent filenames, program names and commands. For example: **use the copy command**.
`Boldface Typewriter Font`	Indicates commands and responses to prompts that must be typed exactly as printed in the manual.
Initial capital letter	Indicates a window name. Names of keys on the keyboard have initial capitals. For example: Click Enter.
Menu Name > Menu Option	**Menu Name > Menu Option** Indicates the menu structure. **Device > Port > Port Properties** means the Port Properties menu option under the Port menu option that is located under the Device menu.

Notes, Cautions, and Warnings

NOTE

A NOTE indicates important information that helps make better use of the device.

CAUTION

A CAUTION indicates either potential damage to hardware or loss of data and tells how to avoid the problem.

WARNING!

A WARNING indicates a potential for property damage, personal injury, or death.

1 Web-based (GUI) Configuration

CHAPTER

Introduction

All software functions of the Switch can be managed, configured and monitored via the embedded web-based (HTML) interface. The Switch can be managed from remote stations anywhere on the network through a standard browser such as Mozilla Firefox, Microsoft Internet Explorer. The browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol. For some functions of the web-based configuration, you will need to have the latest version of Java installed in order to display the data correctly.

The Web-based management module and the Console program (and Telnet) are different ways to access the same internal switching software and configure it. Thus, all settings encountered in Web-based management are the same as those found in the console program.

Login to Web Manager

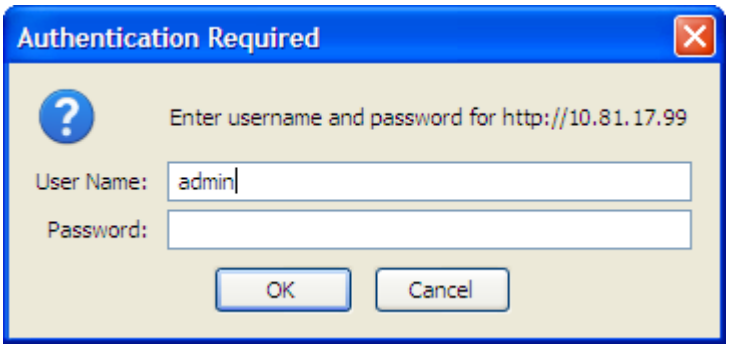
To begin managing the Switch, simply run the browser you have installed on your computer and point it to the IP address you have defined for the device. The URL in the address bar should be in the format: http://123.123.123.123, where the numbers 123 represent the IP address of the Switch.

NOTE

The Factory default IP address for the Switch is 0.0.0.0. The user must first configure an IP address for the Switch through the console port before connecting to the Web Manager.

This opens the management module's user authentication window, as seen below.

Figure 1: Enter Network Password dialog



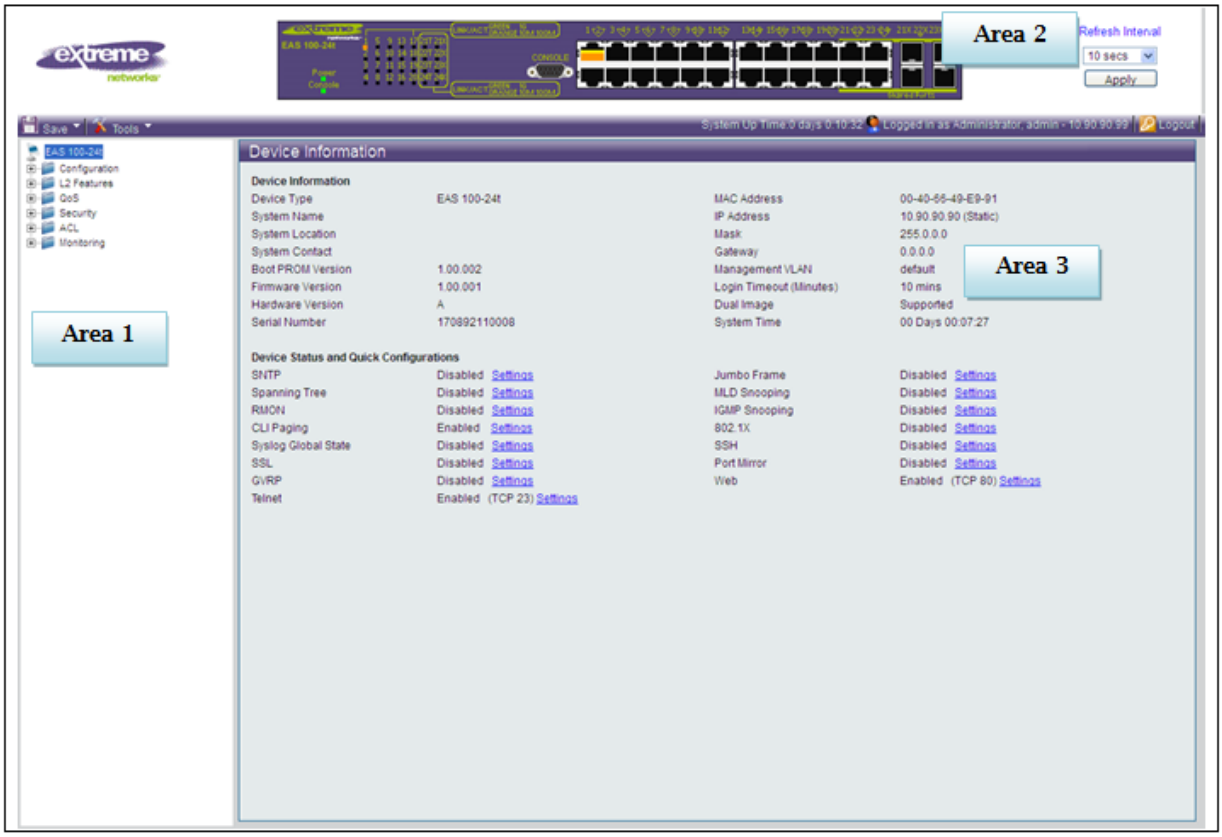
The default User Name is **admin** and Password for this Switch is blank. Click **OK**. This will open the Web-based user interface. The Switch management features available in the web-based manager are explained below.

Web-based User Interface

The user interface provides access to various Switch configuration and management windows, allows you to view performance statistics, and permits you to graphically monitor the system status.

Areas of the User Interface

The figure below shows the user interface. The user interface is divided into three distinct areas as described in the table.



Area 1	Select the folder or window to be displayed. The folder icons can be opened to display the hyperlinked window buttons and subfolders contained within them. Click the Extreme Networks logo to go to the Extreme Networks website.
Area 2	Presents a graphical near real-time image of the front panel of the Switch. This area displays the Switch's ports and expansion modules, showing port activity, duplex mode, or speed, depending on the specified mode. Various areas of the graphic can be selected for performing management functions, including port configuration.
Area 3	Presents switch information based on your selection and the entry of configuration data.

CAUTION

Any changes made to the Switch configuration during the current session must be saved in the **Save Configuration** window (**Save > Save Configuration**) or use the command line interface (CLI) command **save config**.

Web Pages

When you connect to the management mode of the Switch with a Web browser, a login window is displayed. Enter a user name and password to access the Switch's management mode.

Below is a list and description of the main folders available in the Web interface:

- **Configuration** – Contains main windows concerning Device Information, System Information, Serial Port Settings, IP Address Settings, IPv6 Interface Settings, IPv6 Route Settings, IPv6 Neighbor Settings, Port Configuration, Static ARP Settings, User Accounts, System Log Configuration, MAC Address Aging Time, Web Settings, Telnet Settings, CLI Paging Settings, Firmware Information, SNTP Settings, SMTP Settings, and SNMP Settings.
- **L2 Features** – Contains main windows concerning Jumbo Frame, 802.1Q Static VLAN, Q-in-Q, 802.1v Protocol VLAN, GVRP Settings, Asymmetric VLAN Settings, MAC-based VLAN Settings, PVID Auto Assign Settings, Port Trunking, LACP Port Settings, Traffic Segmentation, IGMP Snooping, MLD Snooping Settings, Port Mirror,Loopback Detection Settings, Spanning Tree, Forwarding & Filtering, and LLDP.
- **QoS** – Contains main windows concerning Bandwidth Control, Traffic Control, 802.1P Default Priority, 802.1P User Priority, QoS Scheduling Settings, Priority Mapping, TOS Mapping, and DSCP Mapping.
- **Security** – Contains main windows concerning Trusted Host, Port Security, 802.1X, SSL Settings, SSH, Access Authentication Control, and MAC-based Access Control Settings.
- **ACL** – Contains main windows concerning ACL Configuration Wizard, Access Profile List, ACL Finder, and ACL Flow Meter.
- **Monitoring** – Contains main windows concerning Cable Diagnostics, CPU Utilization, Port Utilization, Packet Size, Memory Utilization, Packets, Errors, Port Access Control, Browse ARP Table, Browse VLAN, IGMP Snooping, MLD Snooping, LLDP, MBA Authentication State, Browse Session Table, MAC Address Table, and System Log.
- **Save & Tools** – Contains main windows concerning Save Configuration, Save Log, Save All, Configuration File Upload & Download, Upload Log File, Reset, Ping Test, Download Firmware, and Reboot System.

NOTE

Ensure that you have configured the user name and password in the **User Accounts** window (**Configuration > User Accounts**) before connecting the Switch to the greater network.

2 Configuration

CHAPTER

Device Information

This window contains the main settings for all major functions on the Switch and appears automatically when you log on. To return to the **Device Information** window, click the **EAS 100-24t** folder. The **Device Information** window shows the Switch's MAC Address (assigned by the factory and unchangeable), the Boot PROM Version, Firmware Version and other information about different settings on the Switch.

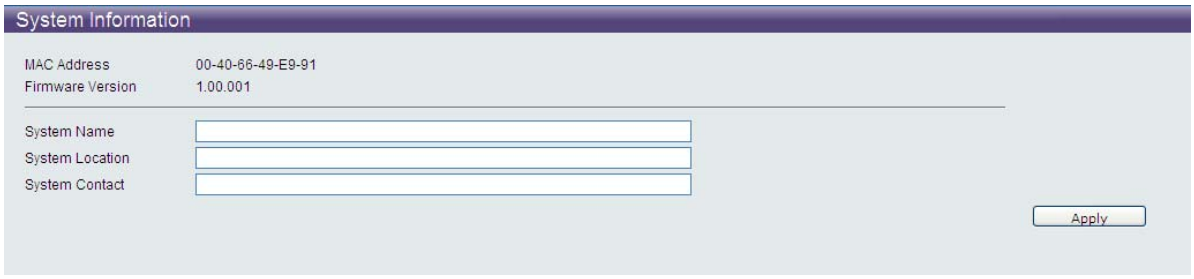
This information is helpful to keep track of PROM and firmware updates and to obtain the Switch's MAC address for entry into another network device's address table if necessary. In addition, this window displays the status of functions on the Switch to quickly assess their status.

Some functions are hyper-linked to their configuration window for easy access from the **Device Information** window.

System Information

This window contains the System Information details. The user may enter a System Name, System Location and System Contact to aid in defining the Switch, to the user's preference. This window displays the MAC Address, and Firmware Version.

Click **Configuration > System Information** to display the following window:



In this window, the following parameters can be configured:

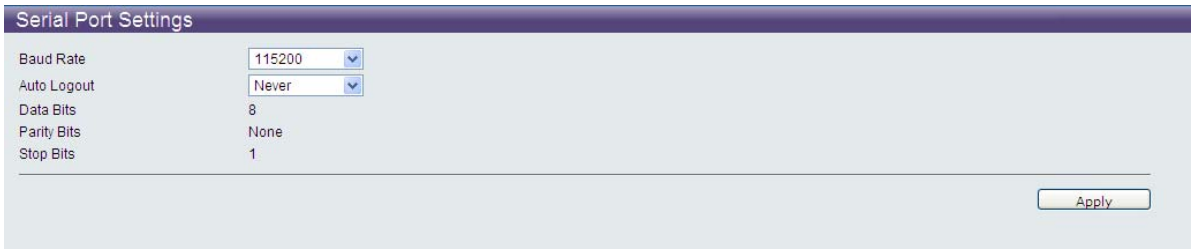
Parameter	Description
System Name	The name which identifies the switch in the Switch network.
System Location	The location where the Switch is stored.
System Contact	A contact name or number in the event that maintenance or support is required.

Click on the **Apply** button to accept the changes made.

Serial Port Settings

The following window allows the Baud Rate and the Auto Logout to be changed as well as containing information about the Serial Port Settings.

Click **Configuration > Serial Port Settings** to display this window:



In this window, the following parameters can be configured:

Parameter	Description
Baud Rate	This field specifies the baud rate for the serial port on the Switch. There are four possible baud rates to choose from, *9600*, *19200*, *38400* and *115200.* The default setting is *9600*.
Auto Logout	Select the logout time used for the console interface. This automatically logs the user out after an idle period of time as defined. Choose from the following options: *2 Minutes, 5 Minutes, 10 Minutes, 15 Minutes* or *Never*. The default setting is *10 minutes*.

Click on the **Apply** button to accept the changes made.

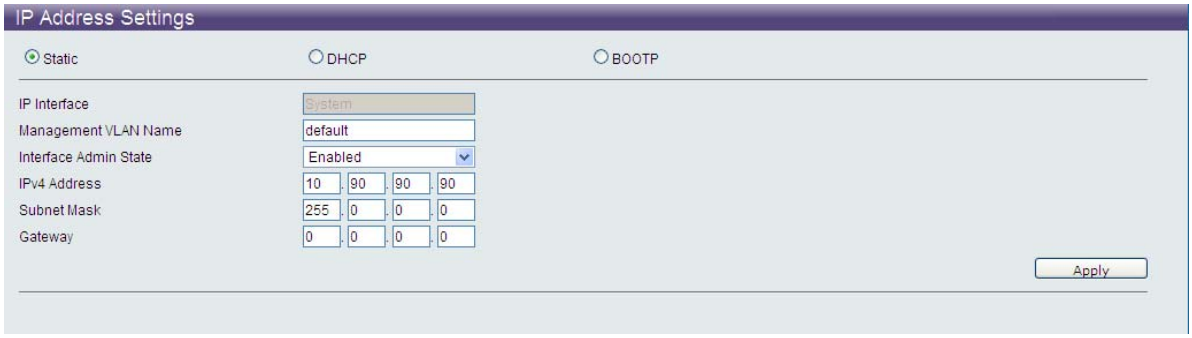
NOTE

If a user configures the serial port's baud rate, the baud rate will take effect and save immediately.

IP Address Settings

The IP address may initially be set using the console interface prior to connecting to it through the Ethernet. If the Switch IP address has not yet been changed, refer to the introduction of the *Extreme Networks EAS 100-24t CLI Manual* for more information.

Click **Configuration > IP Address Settings** to display the following window:



To manually assign the Switch's IP address, subnet mask, and default gateway address:

1. Select the *Static* radio button.
2. Enter the appropriate IPv4 Address and Subnet Mask.
3. To access the Switch from a different subnet than the one it is installed on, enter the IP address of the Gateway. If the Switch will be managed from the subnet on which it is installed, leave the default address (0.0.0.0) in this field.
4. If no VLANs have been previously configured on the Switch, you can use the *default* Management VLAN Name. The *default* VLAN contains all of the Switch ports as members. If VLANs have been previously configured on the Switch, the Management VLAN Name of the VLAN that contains the port connected to the management station will have to be entered to access the Switch.
5. Use the drop-down Interface Admin State menu to select *Enabled* if it has not already been done.

NOTE

The Switch's factory default IP address is 0.0.0.0 with a subnet mask of 255.0.0.0 and a default gateway of 0.0.0.0. To access the web configuration, the you must first configure an IP address for the Switch using the Console Connection.

To use the BOOTP or DHCP protocols to assign the Switch an IP address, subnet mask, and default gateway address, select either *BOOTP* or *DHCP*.

In this window, the following parameters can be configured:

Parameter	Description
Static	Allows the entry of an IPv4 address, Subnet Mask, and a Default Gateway for the Switch. These fields should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal form) between 0 and 255. This address should be a unique address on the network assigned for use by the network administrator.
DHCP	The Switch will send out a DHCP broadcast request when it is powered up. The DHCP protocol allows IP addresses, network masks, and default gateways to be assigned by a DHCP server. If this option is set, the Switch will first look for a DHCP server to provide it with this information before using the default or previously entered settings.
BOOTP	The Switch will send out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the Switch will first look for a BOOTP server to provide it with this information before using the default or previously entered settings.
IP Interface	The current IP Interface being assigned an IP address on this window.
Management VLAN Name	This allows the entry of a VLAN Name from which a management station will be allowed to manage the Switch using TCP/IP (in-band via web manager or Telnet). Management stations that are on VLANs other than the one entered here will not be able to manage the Switch in-band unless their IP addresses are entered in the **Security IP Management** window. If VLANs have not yet been configured for the Switch, the default VLAN contains all of the Switch's ports. There are no entries in the Security IP Management table, by default, so any management station that can connect to the Switch can access the Switch until a management VLAN is specified or Management Station IP Addresses are assigned.
Interface Admin State	Toggle between *Enabled* and *Disabled*. This must be set to *Enabled* when setting an IP address on this window.
IPv4 Address	Enter the desired IPv4 address to be set. The default address is *0.0.0.0*.
Subnet Mask	A Bitmask that determines the extent of the subnet that the Switch is on. Should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.
Gateway	IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged.

Click on the **Apply** button to accept the changes made.

Setting the Switch's IP Address using the Console Interface

Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP, TFTP). The Switch's default IP address is 0.0.0.0. The default Switch IP address can be changed to meet the specification of your networking address scheme.

The IP address for the Switch must be set before the Web-based manager can manage the switch. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known. The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:

- Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy.** Where the x letters represent the IP address to be assigned to the IP interface named System and the y letters represent the corresponding subnet mask.
- Alternatively, the user can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z.** Where the x letters represent the IP address to be assigned to the IP interface named **System** and the z represents the corresponding number of subnets in CIDR notation.

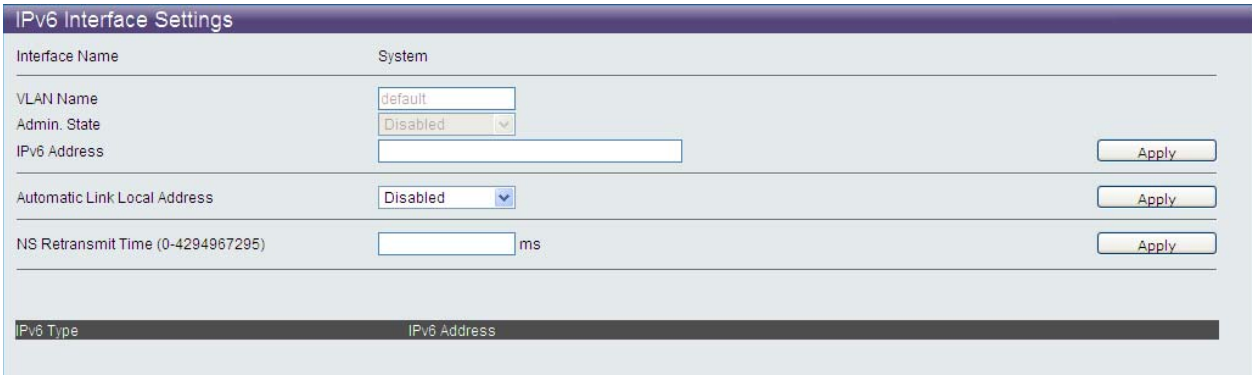
The IP interface named System on the Switch can be assigned an IP address and subnet mask, which can then be used to connect a management station to the Switch's Telnet or Web-based management agent.

Successful entry of the command will produce a "**Success"** message, indicating that the command execution was correct. You may now utilize this address to configure or manage the Switch through Telnet, the Command Line Interface (CLI) or the Web-based management (GUI).

IPv6 Address Settings

You can display the Switch's current IPv6 interface settings.

To view the following window, click **Configuration** > **IPv6 Interface Settings**:



To configure IPv6 interface settings, enter an IPv6 Address and click **Apply**. The new entry will appear in the table at the bottom of the window.

In this window, the following parameters can be configured:

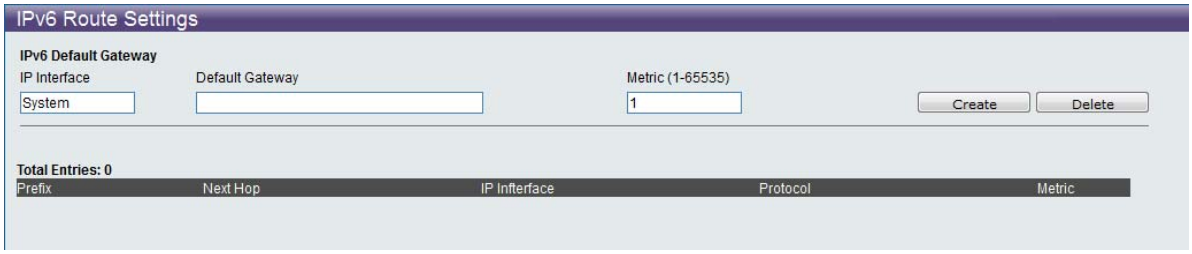
Parameter	Description
Interface Name	The name of the IPv6 interface being displayed or modified.
VLAN Name	Display the VLAN name of the IPv6 interface.
Admin. State	Display the current administrator state.
IPv6 Address	Enter the IPv6 address of the interface to be modified.
Automatic Link Local Address	Toggle between *Enabled* and *Disabled*. Enabling this is helpful when no external source of network addressing information is available.
NS Retransmit Time (0-4294967295)	Enter a value between *0* and *4294967295*. This is the neighbor solicitation's retransmit timer in milliseconds. The default is zero.

Click on the **Apply** button to accept the changes made.

IPv6 Route Settings

The user can configure the Switch's IPv6 Route Table.

To view the following window, click **Configuration > IPv6 Route Settings**:

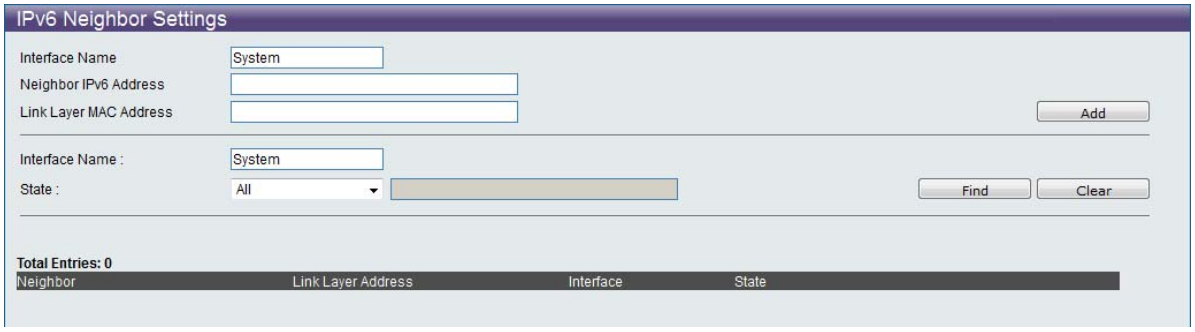


Enter an **IPv6 Interface**, an IPv6 address in the **Default Gateway** field and then click the **Create** button. In addition, the **Metric** can be entered between *1* and *65535*. The new IPv6 route will be displayed in the table at the bottom of the window.

IPv6 Neighbor Settings

You can configure the Switch's IPv6 neighbor settings. The Switch's current IPv6 neighbor settings will be displayed in the table at the bottom of this window.

To view the IPv6 Neighbor Settings, click **Configuration** > **IPv6 Neighbor Settings**:



In this window, the following parameters can be configured:

Parameter	Description
Interface Name	Displays the interface name. This field is not user-configurable. To search for all the current interfaces on the Switch, go to the second Interface Name field in the middle part of the window, tick the All check box, and then click the **Find** button.
Neighbor IPv6 Address	Enter the neighbor IPv6 address.
Link Layer MAC Address	Enter the link layer MAC address.
State	Use the drop-down menu to select *All*, *Address*, *Static*, or *Dynamic*.

Click on the **Add** button to add a new IPv6 Neighbor address and Link Layer MAC Address.

Click on the **Find** button to find the specific entry based on the information entered.

Click on the **Clear** button to remove the entered data from the fields.

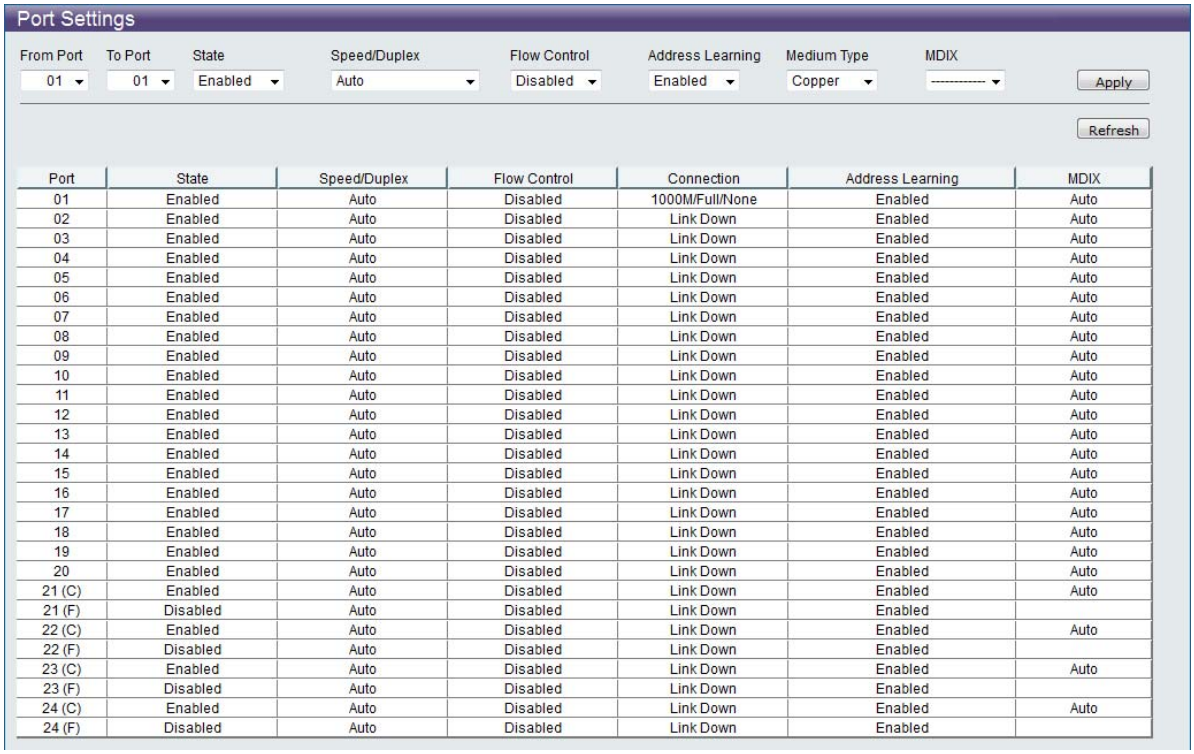
Port Configuration Folder

This section contains information for configuring various attributes and properties for individual physical ports, including port speed and flow control.

Port Settings

Various port settings, including State, Speed/Duplex, Flow Control, Address Learning, Medium Type, and MDIX can be configured on the Switch.

To view the Port Settings window, click **Configuration > Port Configuration > Port Settings**:


Port Settings
From Port
To Port
State
Speed/Duplex
Flow Control
Address Learning
Medium Type
MDIX
01
01
Enabled
Auto
Disabled
Enabled
Copper

Apply
Refresh
Port
State
Speed/Duplex
Flow Control
Connection
Address Learning
MDIX
01 Enabled Auto Disabled 1000M/Full/None Enabled Auto
02 Enabled Auto Disabled Link Down Enabled Auto
03 Enabled Auto Disabled Link Down Enabled Auto
04 Enabled Auto Disabled Link Down Enabled Auto
05 Enabled Auto Disabled Link Down Enabled Auto
06 Enabled Auto Disabled Link Down Enabled Auto
07 Enabled Auto Disabled Link Down Enabled Auto
08 Enabled Auto Disabled Link Down Enabled Auto
09 Enabled Auto Disabled Link Down Enabled Auto
10 Enabled Auto Disabled Link Down Enabled Auto
11 Enabled Auto Disabled Link Down Enabled Auto
12 Enabled Auto Disabled Link Down Enabled Auto
13 Enabled Auto Disabled Link Down Enabled Auto
14 Enabled Auto Disabled Link Down Enabled Auto
15 Enabled Auto Disabled Link Down Enabled Auto
16 Enabled Auto Disabled Link Down Enabled Auto
17 Enabled Auto Disabled Link Down Enabled Auto
18 Enabled Auto Disabled Link Down Enabled Auto
19 Enabled Auto Disabled Link Down Enabled Auto
20 Enabled Auto Disabled Link Down Enabled Auto
21 (C) Enabled Auto Disabled Link Down Enabled Auto
21 (F) Disabled Auto Disabled Link Down Enabled
22 (C) Enabled Auto Disabled Link Down Enabled Auto
22 (F) Disabled Auto Disabled Link Down Enabled
23 (C) Enabled Auto Disabled Link Down Enabled Auto
23 (F) Disabled Auto Disabled Link Down Enabled
24 (C) Enabled Auto Disabled Link Down Enabled Auto
24 (F) Disabled Auto Disabled Link Down Enabled

To configure switch ports, choose the port or sequential range of ports using the From Port and To Port pull-down menus.

In this window, the following parameters can be configured:

Parameter	Description
From Port/To Port	Use the pull-down menus to select the port or range of ports to be configured.
State	Toggle this field to either enable or disable a given port or group of ports.

Parameter	Description
Speed/Duplex	Toggle the **Speed/Duplex** field to either select the speed and duplex/half-duplex state of the port. *Auto* denotes auto-negotiation between 10/100/1000 Mbps devices, in full-duplex or half-duplex. The *Auto* setting allows the port to automatically determine the fastest settings between the connected devices and to use those settings. The other options are *Auto*, *10M Half*, *10M Full, 100M Half* and *100M Full*, *1000M Full_Master, 1000M Full_Slave* and *1000M Full*. There is no automatic adjustment of port settings with any option other than *Auto*. The Switch allows the user to configure two types of gigabit connections; *1000M/Full_M* and *1000M/Full_S*. Gigabit connections only support full duplex connections and take on certain characteristics that are different from the other choices listed. The *1000M Full_Master* and *1000M Full_Slave* parameters refer to connections running a 1000BASE-T cable for connection between the Switch port and other device capable of a gigabit connection. The master setting (*1000M Full_Master)* will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source. The slave setting (*1000M Full_Slave)* uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for *1000M Full_Master*, the other side of the connection must be set for *1000M Full_Slave*. Any other configuration will result in a link down status for both ports.
Flow Control	Displays the flow control scheme used for the various port configurations. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control, and *Auto* ports use an automatic selection of the two. The default is *Disabled*.
Address Learning	When *Enabled*, destination and source MAC addresses are automatically listed in the forwarding table. The default setting is *Enabled*.
Medium Type	This applies only to the Combo ports. The command is available for the user to enable or disable the port with the specified medium type. When one medium type specified is enabled, the other medium type is disabled implicitly. That is, each of the two types of the transport medium shall be enabled exclusively. Both of the medium types of a specified port can be disabled at the same time. The Copper port is selected (enabled) by default.
MDIX	This can be specified as *Auto*, *Normal*, or *Cross*. In *Normal* state, the port is in MDIX mode and can be connected to a PC NIC using a straight cable. If it is in *Cross* state, the port is in MDI mode, and can be connected to a port (in MDIX mode) on another switch through a straight cable.

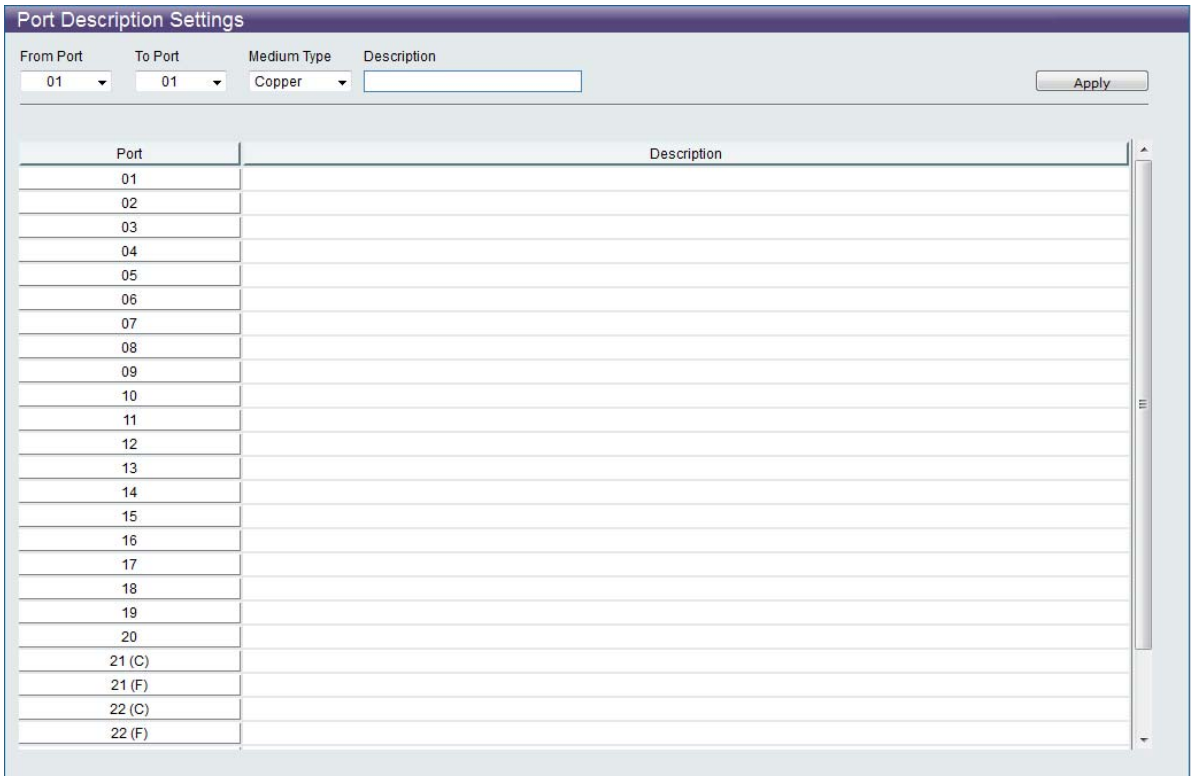
Click on the **Apply** button to accept the changes made.

Click on the **Refresh** button to refresh the display list.

Port Description Settings

The Switch supports a port description feature where the user may name various ports on the Switch.

To view the Port Description Settings window, click **Configuration > Port Configuration > Port Description Settings**:



Use the **From Port** and **To Port** pull-down menus to choose a port or range of ports to describe, and then enter a description of the port(s).

The Medium Type applies only to the Combo ports. If configuring the Combo ports this defines the type of transport medium used. SFP ports should be nominated *Fiber* and the Combo 1000BASE-T ports should be nominated *Copper*. The result will be displayed in the appropriate switch port number slot (C for copper ports and F for fiber ports).

In this window, the following parameters can be configured:

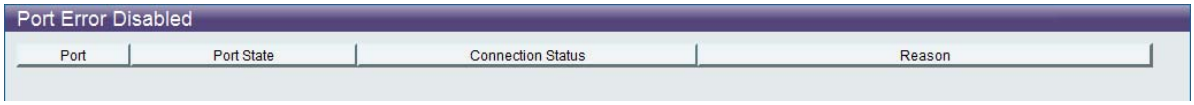
Parameter	Description
From Port/To Port	Use the pull-down menus to select the port or range of ports to be configured.
Medium Type	This only applies to the Combo ports. If configuring the Combo ports, this defines the type of transport medium used. SFP ports should be set at *Fiber* and the Combo 1000BASE-T ports should be set at *Copper*.
Description	Enter a string into the Description field to provide some information about the port.

Click on the **Apply** button to accept the changes made.

Port Error Disabled

The following window will display information about ports that have had their connection status disabled for reasons such as loopback detection or Traffic Control.

To view this window, click **Configuration > Port Configuration > Port Error Disabled**:



In this window, the following parameters can be configured:

Parameter	Description
Port	Displays the port that has been error disabled.
Port State	Describes the current running state of the port.
Connection Status	This field will read the uplink status of the individual ports.
Reason	Describes the reason why the port has been error-disabled, such as a loopback occurrence.

Port Media Type

The following window will display information about the port media type.

To view this window, click **Configuration > Port Configuration > Port Media Type**:

Port Media Type

Port	Type
01	1000BASE-T
02	1000BASE-T
03	1000BASE-T
04	1000BASE-T
05	1000BASE-T
06	1000BASE-T
07	1000BASE-T
08	1000BASE-T
09	1000BASE-T
10	1000BASE-T
11	1000BASE-T
12	1000BASE-T
13	1000BASE-T
14	1000BASE-T
15	1000BASE-T
16	1000BASE-T
17	1000BASE-T
18	1000BASE-T
19	1000BASE-T
20	1000BASE-T
21	1000BASE-T
22	1000BASE-T
23	1000BASE-T
24	1000BASE-T

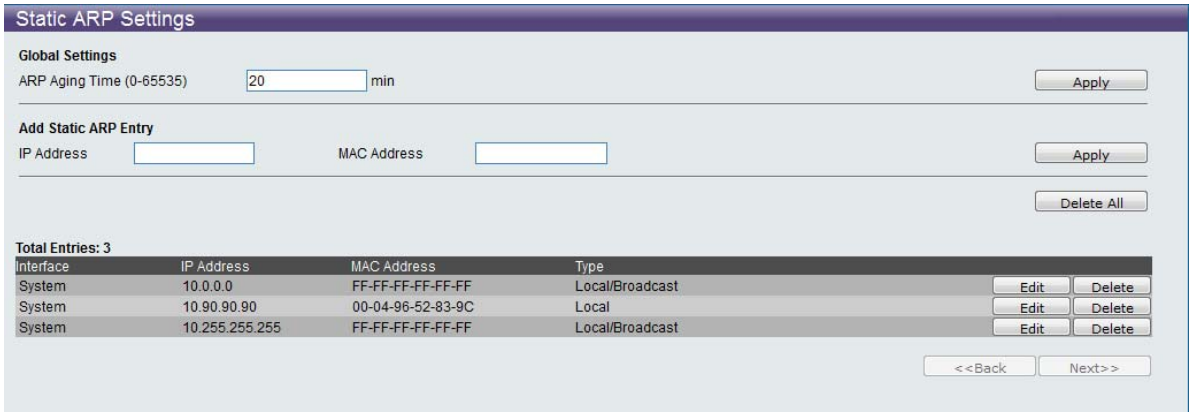
In this window, the following parameters can be configured:

Parameter	Description
Port	Displays the port number to view the corresponding media type.
Type	Displays the medium type of the ports.

Static ARP Settings

The Address Resolution Protocol (ARP) is a TCP/IP protocol that converts IP addresses into physical addresses. This table allows network managers to view, define, modify and delete ARP information for specific devices. Static entries can be defined in the ARP Table. When static entries are defined, a permanent entry is entered and is used to translate IP address to MAC addresses.

To view this window, click **Configuration > Static ARP Settings**:



In this window, the following parameters can be configured:

Parameter	Description
ARP Aging Time (0-65535)	The user may globally set the maximum amount of time, in seconds, that an Address Resolution Protocol (ARP) entry can remain in the Switch's ARP table without being accessed before it is dropped from the table. The value may be set in the range of *0* to *65535* seconds, with a default setting of *20* minutes.
IP Address	The IP address of the ARP entry.
MAC Address	The MAC address of the ARP entry.

After entering the IP Address and MAC Address of the Static ARP entry, click **Apply** to implement the new entry. To completely clear the Static ARP Settings, click the **Delete All** button. To modify a static ARP entry, click the corresponding **Edit** button in the table. To delete a static ARP entry, click the corresponding **Delete** button in the table.

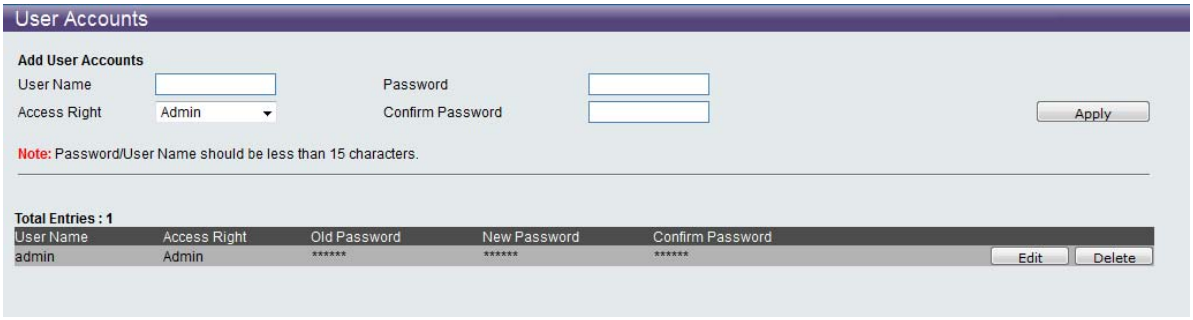
NOTE

The Switch supports up to 255 static ARP entries.

User Accounts

Use this window to control user privileges, create new users, and view existing User Accounts.

To view this window, click **Configuration > User Accounts**:



In this window, the following parameters can be configured:

Parameter	Description
User Name	The name of the user, an alphanumeric string of up to 15 characters.
Password	Enter a password for the new user.
Access Right	There are two levels of user privileges, *Admin* and *User*. Some features and selections available to users with *Admin* privileges may not be available to those with *User* level privileges. (Table 1 below summarizes Admin and User level privileges)
Confirm Password	Retype the new password.

To add a new user, enter the appropriate information and click **Apply**. To modify or delete an existing user, click on the **Edit** button for that user. Click on the **Delete** button to remove the selected entry.

Admin and User Privileges

There are two levels of user privileges, **Admin** and **User**. Some menu selections available to users with **Admin** privileges may not be available to those with **User** privileges.

The following table summarizes the Admin and User privileges:

Table 1: Admin and User Privileges

Management	Admin	User
Configuration	Yes	No
Network Monitoring	Yes	Read-only
Community Strings and Trap Stations	Yes	Read-only
Update Firmware and Configuration Files	Yes	No
System Utilities	Yes	No
Factory Reset	Yes	No
User Account Management	**Admin**	**User**
Add/Update/Delete User Accounts	Yes	No
View User Accounts	Yes	No

System Log Configuration Folder

This section contains information for configuring various attributes and properties for System Log Configurations, including System Log Settings and System Log Host.

System Log Settings

This window allows the user to enable or disable the System Log and specify the System Log Save Mode Settings.

To configure the system log settings, click **Configuration > System Log Configuration > System Log Settings**:

In this window, the following parameters can be configured:

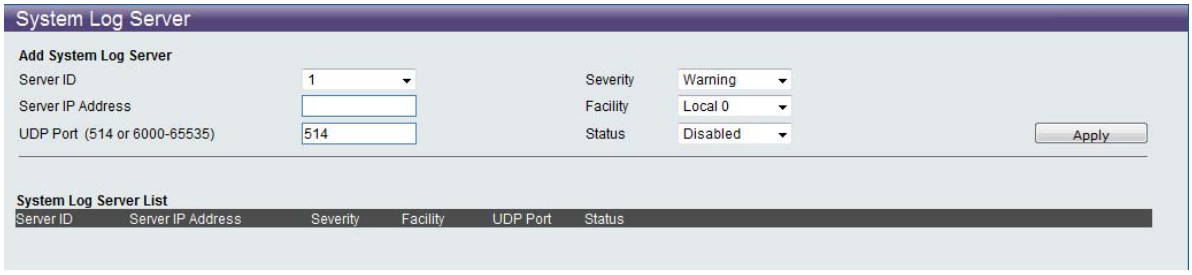
Parameter	Description
System Log	Use the radio buttons to either enable or disable the system log feature.
Save Mode	Use this drop-down menu to choose the method that will trigger a log entry. You may select from *On Demand*, *Time Interval*, and *Log Trigger*.
min (1-65535)	Enter a time interval, in minutes, for which a log entry is to be made.

Click on the **Apply** button to accept the changes made.

System Log Server

The Switch can send Syslog messages to up to four designated servers using the System Log Server.

To configure the system log settings, click **Configuration > System Log Configuration > System Log Server**:



In this window, the following parameters can be configured:

Parameter	Description
Server ID	Syslog server settings index (1-4).
Severity	This drop-down menu allows you to select the level of messages that will be sent. The options are *Warning*, *Informational*, and *All*.
Server IP Address	The IP address of the Syslog server.
Facility	Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: **Bold** font indicates the facility values that the Switch is currently employing.

Numerical	Facility Code	Numerical	Facility Code
0	kernel messages	12	NTP subsystem
1	user-level messages	13	log audit
2	mail system	14	log alert
3	system daemons	15	clock daemon
4	security/authorization messages	16	local use 0 (local0)
5	messages generated internally by syslog	17	local use 1 (local1)
7	line printer subsystem	18	local use 2 (local2)
8	network news subsystem	19	local use 3 (local3)
9	UUCP subsystem	20	local use 4 (local4)
10	clock daemon	21	local use 5 (local5)
11	security/authorization messages	22	local use 6 (local6)
	FTP daemon	23	**local use 7 (local7)**

UDP Port (514 or 6000-65535)	Type the UDP port number used for sending Syslog messages. The default is *514*.
Status	Choose *Enabled* or *Disabled* to activate or deactivate.

Parameter	Description
Server ID	Syslog server settings index (1-4).
Severity	This drop-down menu allows you to select the level of messages that will be sent. The options are *Warning*, *Informational*, and *All*.
Server IP Address	The IP address of the Syslog server.

Parameter	Description
Facility	Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: **Bold** font indicates the facility values that the Switch is currently employing.

Numerical	Facility Code	Numerical	Facility Code
0	kernel messages	12	NTP subsystem
1	user-level messages	13	log audit
2	mail system	14	log alert
3	system daemons	15	clock daemon
4	security/authorization messages	16	local use 0 (local0)
5	messages generated internally by syslog line printer subsystem	17	local use 1 (local1)
		18	local use 2 (local2)
7	network news subsystem	19	local use 3 (local3)
8	UUCP subsystem	20	local use 4 (local4)
9	clock daemon	21	local use 5 (local5)
10	security/authorization messages	22	local use 6 (local6)
11	FTP daemon	23	**local use 7 (local7)**

UDP Port (514 or 6000-65535)	Type the UDP port number used for sending Syslog messages. The default is *514*.
Status	Choose *Enabled* or *Disabled* to activate or deactivate.

Click on the **Apply** button to accept the changes made.

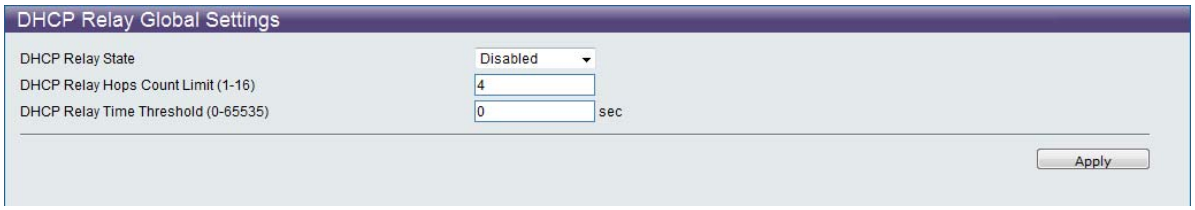
DHCP Relay Folder

This section contains information for configuring various attributes and properties for DHCP Relay Configurations, including DHCP Relay Global and DHCP Relay Interface settings.

DHCP Relay Global Settings

This window allows the user to enable or disable the DHCP Relay State and configure the hop count limit and threshold.

To configure the DHCP Relay Global settings, click **Configuration > DHCP Relay > DHCP Relay Global Settings**:



In this window, the following parameters can be configured:

Parameter	Description
DHCP Relay State:	This option allows the user to enable or disable the DHCP Relay state.
DHCP Relay / Hops Count Limit (1-16):	Enter the maximum number of relay agent hops that the DHCP packets can cross. This value must be between 1 and 16. The default value is 4.
DHCP Relay Time Threshold (0-65535):	Enter the DHCP Relay time threshold value here. If this time is exceeded; the Switch will not relay the DHCP packet. This value must be between 0 and 65535. The default value is 0.

Click on the **Apply** button to accept the changes made.

DHCP Relay Interface Settings

This window allows the user to configure the DHCP Relay Interface Settings.

To configure the DHCP Relay Interface Settings, click **Configuration > DHCP Relay > DHCP Relay Interface Settings**:

In this window, the following parameters can be configured:

Parameter	Description
Interface:	The name of the IP interface for which to display the current DHCP relay configuration.
Server IP:	Enter the DHCP Server IP address here.

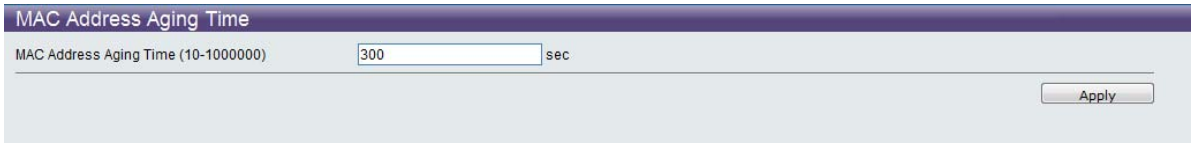
Click on the **Apply** button to accept the changes made.

Click on the **Delete** button to remove the selected entry.

MAC Address Aging Time

This table specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). To change this, enter a value representing the MAC address age-out time in seconds. The MAC Address Aging Time can be set to any value between *10* and *1,000,000* seconds. The default setting is *300* seconds.

To access this window, click **Configuration > MAC Address Aging Time**:



In this window, the following parameters can be configured:

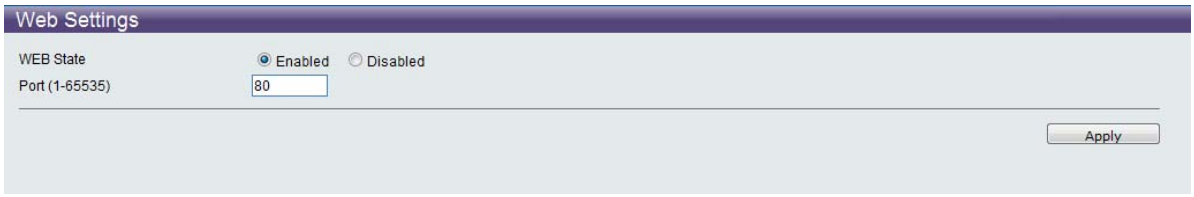
Parameter	Description
MAC Address Aging Time	Specifies the MAC address aging time here. This value must be between 10 and 1000000 seconds. The default value is 300 seconds.

Click on the **Apply** button to accept the changes made.

Web Settings

Web-based management is Enabled by default. If you choose to disable this by selecting Disabled, you will lose the ability to configure the system through the Web interface as soon as these settings are applied. The TCP ports are numbered between *1* and *65535*. The standard TCP port for the Web protocol is *80*.

To access this window, click **Configuration > Web Settings**:



In this window, the following parameters can be configured:

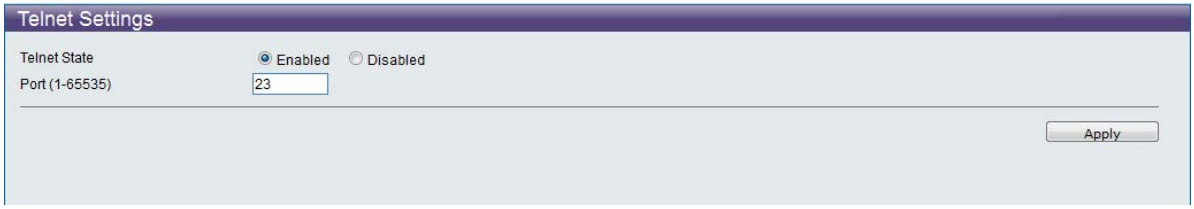
Parameter	Description
WEB State	Specifies to enable or disable the Web settings state.
Port	Specifies the port number used for the Web settings. This value must be between 1 and 65535. The default value is port 80.

Click on the **Apply** button to accept the changes made.

Telnet Settings

Telnet configuration is Enabled by default. If you do not want to allow configuration of the system through Telnet choose Disabled. The TCP ports are numbered between *1* and *65535*. The standard TCP port for the Telnet protocol is *23*.

To access this window, click **Configuration > Telnet Settings**:



In this window, the following parameters can be configured:

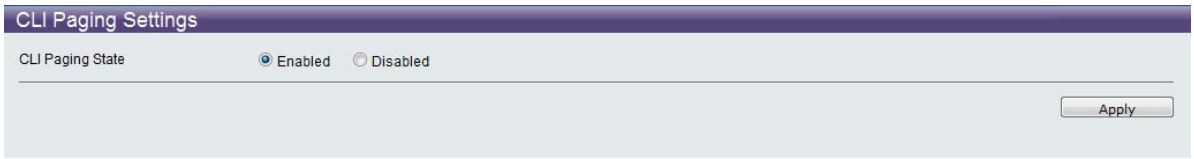
Parameter	Description
Telnet State	Specifies to enable or disable the Telnet settings state.
Port	Specifies the port number used for the Web settings. This value must be between 1 and 65535. The default value is port 23.

Click on the **Apply** button to accept the changes made.

CLI Paging Settings

CLI paging can be Enabled or Disabled in this window. It is **Enabled** by default. CLI paging settings are used when issuing a command which causes the console screen to rapidly scroll through several pages. This command will cause the console to pause at the end of each page.

To access this window, click **Configuration > CLI Paging Settings**:



In this window, the following parameters can be configured:

Parameter	Description
CLI Paging State	Specifies to enable or disable the CLI Paging settings state.

Click on the **Apply** button to accept the changes made.

Firmware Information

Information about current firmware images stored on the Switch can be viewed.

To access this window, click **Configuration > Firmware Information**:

In this window, the following parameters can be configured:

Parameter	Description
ID	States the image ID number of the firmware in the Switch's memory. The Switch can store two firmware images for use. Image ID 1 will be the default boot up firmware for the Switch unless otherwise configured by the user.
Version	States the firmware version.
Size (Bytes)	States the size of the corresponding firmware, in bytes.
Update Time	States the specific time the firmware version was downloaded to the Switch.
From	States the IP address of the origin of the firmware.
User	States the user who downloaded the firmware. This field may read "Anonymous" or "Unknown" for users that are unidentified.

Click on the **Boot UP** button to set the specific firmware as the boot-up firmware.

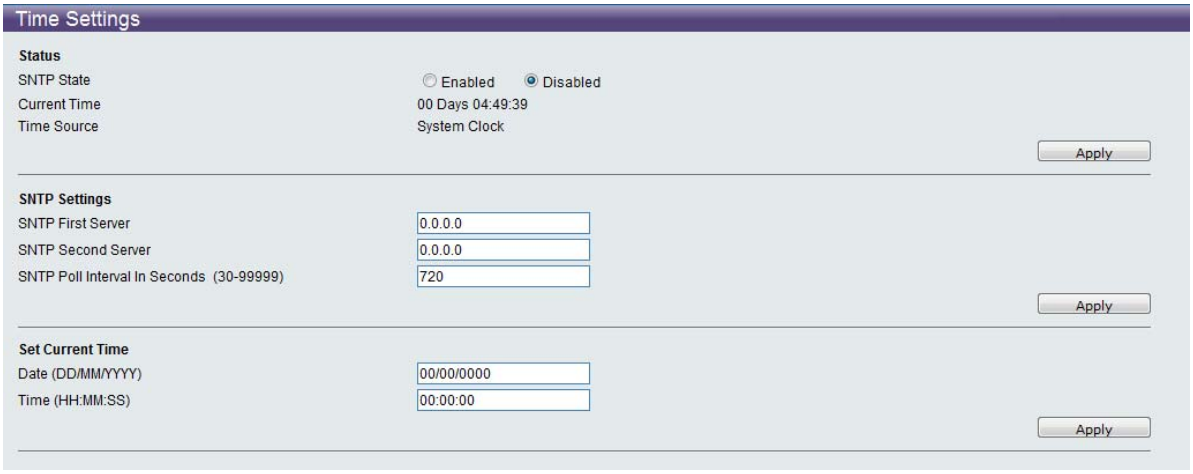
Click on the **Delete** button to remove the selected firmware version.

SNTP Settings Folder

The SNTP Settings folder offers two windows: **Time Settings** and **Time Zone Settings**.

Time Settings

To configure the time settings for the Switch, click **Configuration > SNTP Settings > Time Settings**:



In this window, the following parameters can be configured:

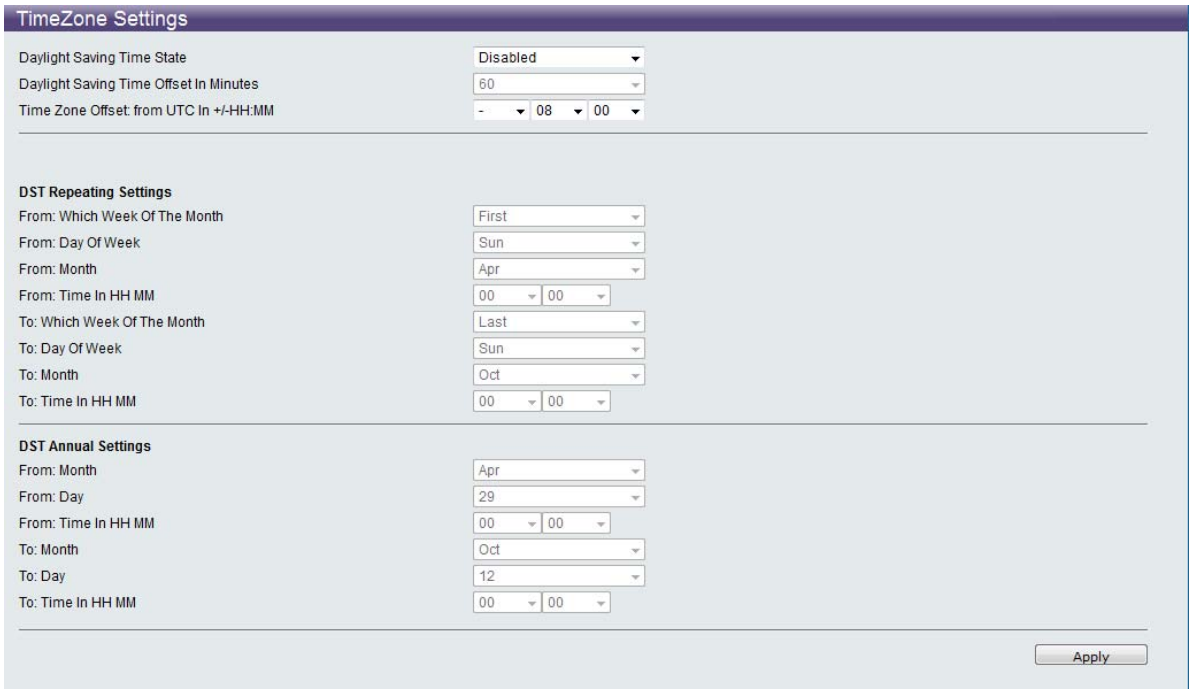
Parameter	Description
Status:	
SNTP State	Use the radio button to select an Enabled or Disabled SNTP state.
Current Time	Displays the Current Time set on the Switch.
Time Source	Displays the time source for the system.
SNTP Settings:	
SNTP First Server	This is the IP address of the primary server the SNTP information will be taken from.
SNTP Second Server	This is the IP address of the secondary server the SNTP information will be taken from.
SNTP Poll Interval in Seconds (30-99999)	This is the interval, in seconds, between requests for updated SNTP information.
Set Current Time:	
Date (DD/MM/YYYY)	Enter the current date in day, month and year to update the system clock.
Time (HH:MM:SS)	Enter the current time in hours, minutes, and seconds.

Click on the **Apply** button to accept the changes made.

Time Zone Settings

The following window is used to configure time zones and Daylight Savings Time settings for SNTP.

To configure the time zone settings for the Switch, click **Configuration > SNTP Settings > Time Zone Settings**:



In this window, the following parameters can be configured:

Parameter	Description
Time Zone and DST:	
Daylight Saving Time State	Use this pull-down menu to enable or disable the DST Settings.
Daylight Saving Time Offset in Minutes	Use this pull-down menu to specify the amount of time that will constitute your local DST offset *30*, *60*, *90*, or *120* minutes.
Time Zone Offset from UTC in +/- HH:MM	Use these pull-down menus to specify your local time zone's offset from Coordinated Universal Time (UTC).
DST Repeating Settings:	
Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October.	
From: Which Week of the Month	Enter the week of the month that DST will start on.
From: Day of the Week	Enter the day of the week that DST will start on.
From: Month	Enter the month DST will start on.
From: Time in HH:MM	Enter the time of day that DST will start on.
To: Which Week of the Month	Enter the week of the month the DST will end.
To: Day of the Week	Enter the day of the week that DST will end.
To: Month	Enter the month that DST will end.
To: Time in HH:MM	Enter the time DST will end.

Parameter	Description
DST Annual Settings	
Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14.	
From: Month	Enter the month DST will start on, each year.
From: Day	Enter the day DST will start on, each year.
From: Time in HH:MM	Enter the time of day DST will start on, each year.
To: Month	Enter the month DST will end, each year.
To: Day	Enter the date DST will end, each year.
To: Time in HH:MM	Enter the time of day that DST will end, each year.

Click on the **Apply** button to accept the changes made.

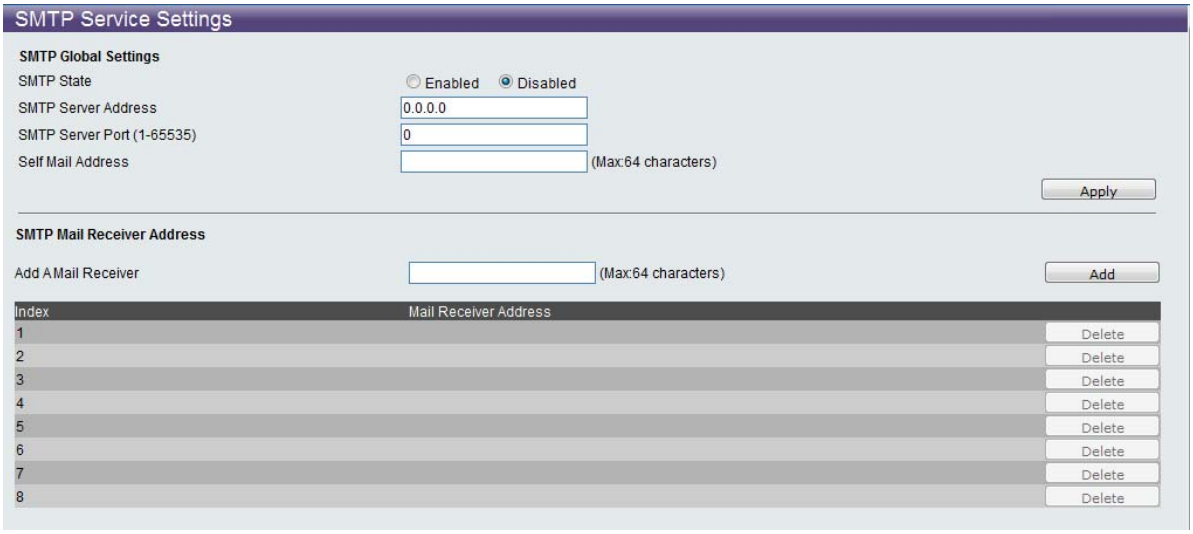
SMTP Settings Folder

SMTP or Simple Mail Transfer Protocol is a function of the Switch that will send switch events to mail recipients based on e-mail addresses entered in the window below. The Switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the Switch, place the appropriate information into an e-mail and deliver it to recipients configured on the Switch. This can benefit the Switch administrator by simplifying the management of small workgroups or wiring closets, increasing the speed of handling emergency Switch events, and enhancing security by recording questionable events occurring on the Switch.

Users can set up the SMTP server for the Switch, along with setting e-mail addresses to which switch log files can be sent when a problem arises on the Switch.

SMTP Service Settings

To view the following window, click **Configuration > SMTP Settings > SMTP Service Settings:**



In this window, the following parameters can be configured:

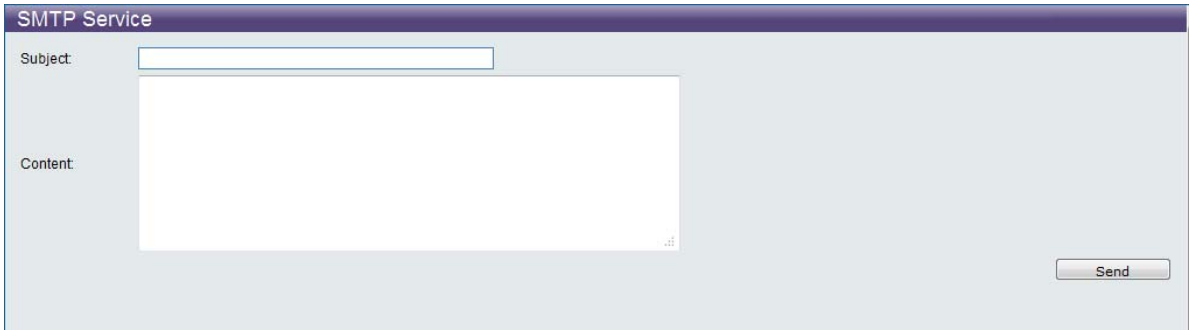
Parameter	Description
SMTP State	Use the radio button to enable or disable the SMTP service on this device.
SMTP Server Address	Enter the IP address of the SMTP server on a remote device. This will be the device that sends out the mail for you.
SMTP Server Port (1-65535)	Enter the virtual port number that the Switch will connect with on the SMTP server. The common port number for SMTP is *25*, yet a value between *1* and *65535* can be chosen.
Self Mail Address	Enter the e-mail address from which mail messages will be sent. This address will be the "from" address on the e-mail message sent to a recipient. Only one self-mail address can be configured for this Switch. This string can be no more that 64 alphanumeric characters.
Add A Mail Receiver	Enter an e-mail address and click the **Add** button. Up to eight e-mail addresses can be added per Switch. To delete these addresses from the Switch, click the corresponding **Delete** button in the SMTP Mail Receiver Address table at the bottom of the window.

Click on the **Apply** button to accept the changes made.

SMTP Service

This window is used to test the SMTP Service Settings configured in the previous window.

To view the following window, click **Configuration > SMTP Settings > SMTP Service**:



To test to see if the SMTP settings are working properly, enter a Subject, Content, and then click the **Send** button.

SNMP Settings Folder

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch, switch group or network.

Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The Switch supports the SNMP versions 1, 2c, and 3. Choose which version to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

In SNMP v.1 and v.2, user authentication is accomplished using 'community strings', which function like passwords. The remote user SNMP application and the Switch SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored (dropped).

The default community strings for the Switch used for SNMP v.1 and v.2 management access are:

- **public** - Allows authorized management stations to retrieve MIB objects.
- **private** - Allows authorized management stations to retrieve and modify MIB objects.

SNMPv3 uses a more sophisticated authentication process that is separated into two parts. The first part is to maintain a list of users and their attributes that are allowed to act as SNMP managers. The second part describes what each user on that list can do as an SNMP manager.

The Switch allows groups of users to be listed and configured with a shared set of privileges. The SNMP version may also be set for a listed group of SNMP managers. Thus, you may create a group of SNMP managers that are allowed to view read-only information or receive traps using SNMPv1 while assigning a higher level of security to another group, granting read/write privileges using SNMPv3.

Using SNMPv3 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions. The functions allowed or restricted are defined using the Object Identifier (OID) associated with a specific MIB. An additional layer of security is available for SNMPv3 in that SNMP messages may be encrypted. To read more about how to configure SNMPv3 settings for the Switch read the next section.

Traps

Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like a port status change. The Switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, and Topology Change.

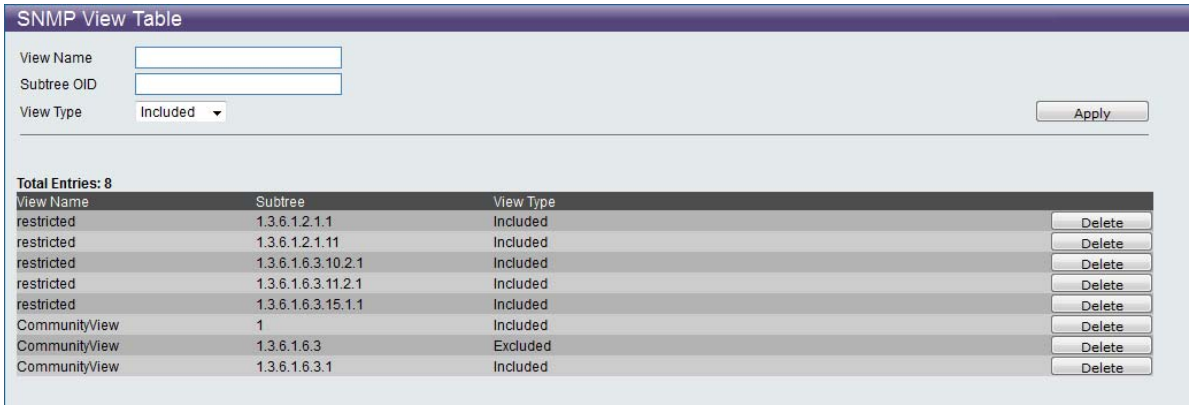
The Switch incorporates a flexible SNMP management for the switching environment. SNMP management can be customized to suit the needs of the networks and the preferences of the network administrator.

The Switch supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The administrator can specify the SNMP version used to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

SNMP View Table

This window is used to assign views to community strings or SNMP groups that define which MIB objects can be accessed by a remote SNMP manager.

To configure SNMP View Settings for the Switch, click **Configuration > SNMP Settings > SNMP View Table**:



In this window, the following parameters can be configured:

Parameter	Description
View Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP view being created.
Subtree OID	Type the Object Identifier (OID) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.
View Type	Select *Included* to include this object in the list of objects that an SNMP manager can access. Select *Excluded* to exclude this object from the list of objects that an SNMP manager can access.

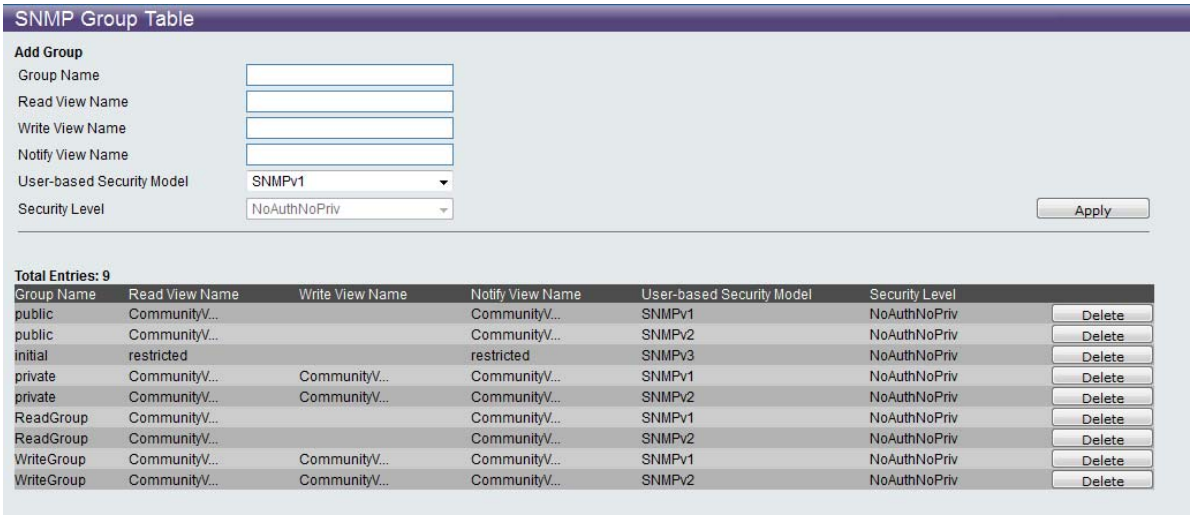
Click on the **Apply** button to accept the changes made.

Click on the **Delete** button to remove the selected entry.

SNMP Group Table

An SNMP Group created with this table maps SNMP users (identified in the **SNMP User Table** window) or community strings to the views created in the previous window.

To view this window, click **Configuration > SNMP Settings > SNMP Group Table**:



In this window, the following parameters can be configured:

Parameter	Description
Group Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP group of SNMP users.
Read View Name	Specify an SNMP group name for users that are allowed SNMP read privileges to the Switch's SNMP agent.
Write View Name	Specify an SNMP group name for users that are allowed SNMP write privileges to the Switch's SNMP agent.
Notify View Name	Specify an SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent.
User-based Security Model	*SNMPv1* - Specifies that SNMP version 1 will be used. *SNMPv2* - Specifies that SNMP version 2c will be used. The SNMPv2 supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *SNMPv3* - Specifies that the SNMP version 3 will be used. SNMPv3 provides secure access to devices through a combination of authentication and encrypting packets over the network.
Security Level	The Security Level settings only apply to SNMPv3. *NoAuthNoPriv* - Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *AuthNoPriv* - Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. *AuthPriv* - Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.

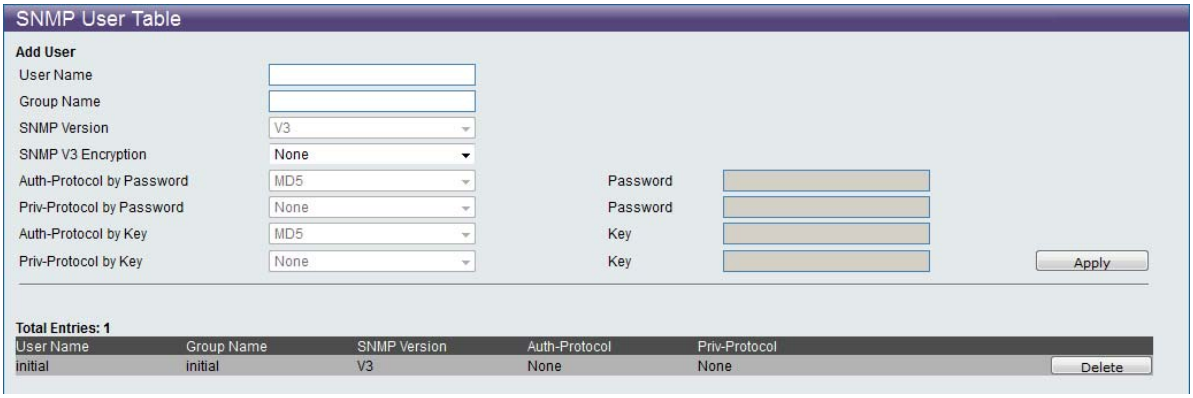
Click on the **Apply** button to accept the changes made.

Click on the **Delete** button to remove the selected entry.

SNMP User Table

This window displays all of the SNMP User's currently configured on the Switch and also allows you to add new users.

To view this window, click **Configuration > SNMP Settings > SNMP User Table**:



In this window, the following parameters can be configured:

Parameter	Description
User Name	An alphanumeric string of up to 32 characters. This is used to identify the SNMP users.
Group Name	This name is used to specify the SNMP group created can request SNMP messages.
SNMP Version	*V1* - Indicates that SNMP version 1 is in use. *V2* - Indicates that SNMP version 2 is in use. *V3* - Indicates that SNMP version 3 is in use.
SNMP V3 Encryption	*None* – Indicates that there is no SNMP V3 Encryption *Password* – Indicates that there is SNMP V3 Encryption through a password *Key* – Indicates that there is SNMP V3 Encryption through a key.
Auth-Protocol by Password	*MD5* - Indicates that the HMAC-MD5-96 authentication level will be used. *SHA* - Indicates that the HMAC-SHA authentication protocol will be used.
Priv-Protocol by Password	*None* - Indicates that no authorization protocol is in use. *DES* - Indicates that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard.
Auth-Protocol by Key	*MD5* - Indicates that the HMAC-MD5-96 authentication level will be used. *SHA* - Indicates that the HMAC-SHA authentication protocol will be used.
Priv-Protocol by Key	*None* - Indicates that no authorization protocol is in use. *DES* - Indicates that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard.
Password	Enter a Password when SNMP V3 Encryption is enabled for Password mode.
Key	Enter a Key when SNMP V3 Encryption is enabled for Key mode.

Click on the **Apply** button to accept the changes made.

Click on the **Delete** button to remove the selected entry.

SNMP Community Table

Use this table to view existing SNMP Community Table configurations and to create a SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string:

- Any MIB view that defines the subset of all MIB objects will be accessible to the SNMP community.
- Read/write or read-only level permission for the MIB objects accessible to the SNMP community.

To configure SNMP Community entries, click **Configuration > SNMP Settings > SNMP Community Table**:

In this window, the following parameters can be configured:

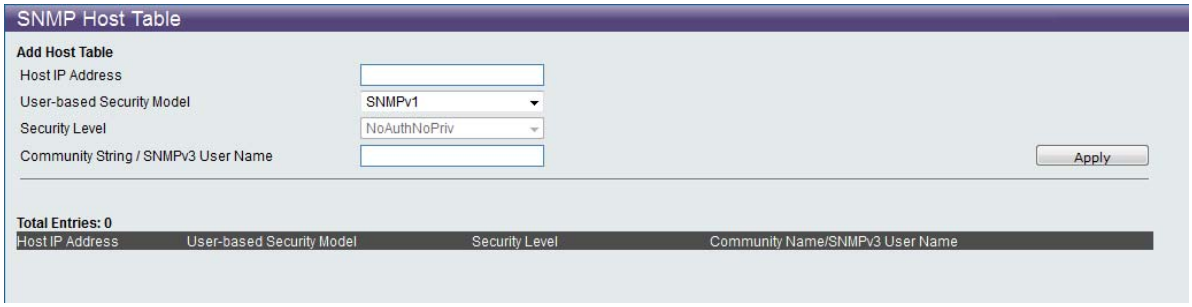
Parameter	Description
Community Name	Type an alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
View Name	Type an alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. The view name must exist in the SNMP View Table.
Access Right	*Read Only* - Specifies that SNMP community members using the community string created can only read the contents of the MIBs on the Switch. *Read Write* - Specifies that SNMP community members using the community string created can read from, and write to the contents of the MIBs on the Switch.

Click on the **Apply** button to accept the changes made.

Click on the **Delete** button to remove the selected entry.

SNMP Host Table

Use the **SNMP Host Table** window to set up SNMP trap recipients. To configure SNMP Host Table entries, click **Configuration > SNMP Settings > SNMP Host Table**



In this window, the following parameters can be configured:

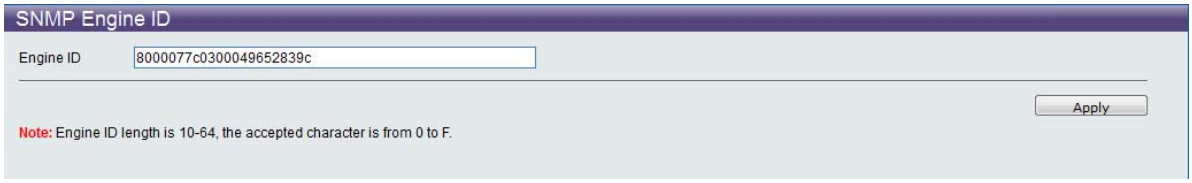
Parameter	Description
Host IP Address	Type the IP address of the remote management station that will serve as the SNMP host for the Switch.
User-based Security Model	*SNMPv1* - Specifies that SNMP version 1 will be used. *SNMPV2c* - Specifies that SNMP version 2 will be used. *SNMPV3* - To specify that the SNMP version 3 will be used.
Security Level	*NoAuthNoPriv* – To specify a NoAuthNoPriv security level. *AuthNoPriv* - To specify an AuthNoPriv security level. *AuthPriv* - To specify an AuthPriv security level.
Community String/ SNMPv3 User Name	Type in the community string or SNMPv3 user name as appropriate.

Click on the **Apply** button to accept the changes made.

SNMP Engine ID

The Engine ID is a unique identifier used for SNMP V3 implementations. This is an alphanumeric string used to identify the SNMP engine on the Switch.

To display the Switch's SNMP Engine ID, click **Configuration > SNMP Settings > SNMP Engine ID**:


SNMP Engine ID
Engine ID
8000077c0300049652839c
Apply
Note: Engine ID length is 10-64, the accepted character is from 0 to F.

In this window, the following parameters can be configured:

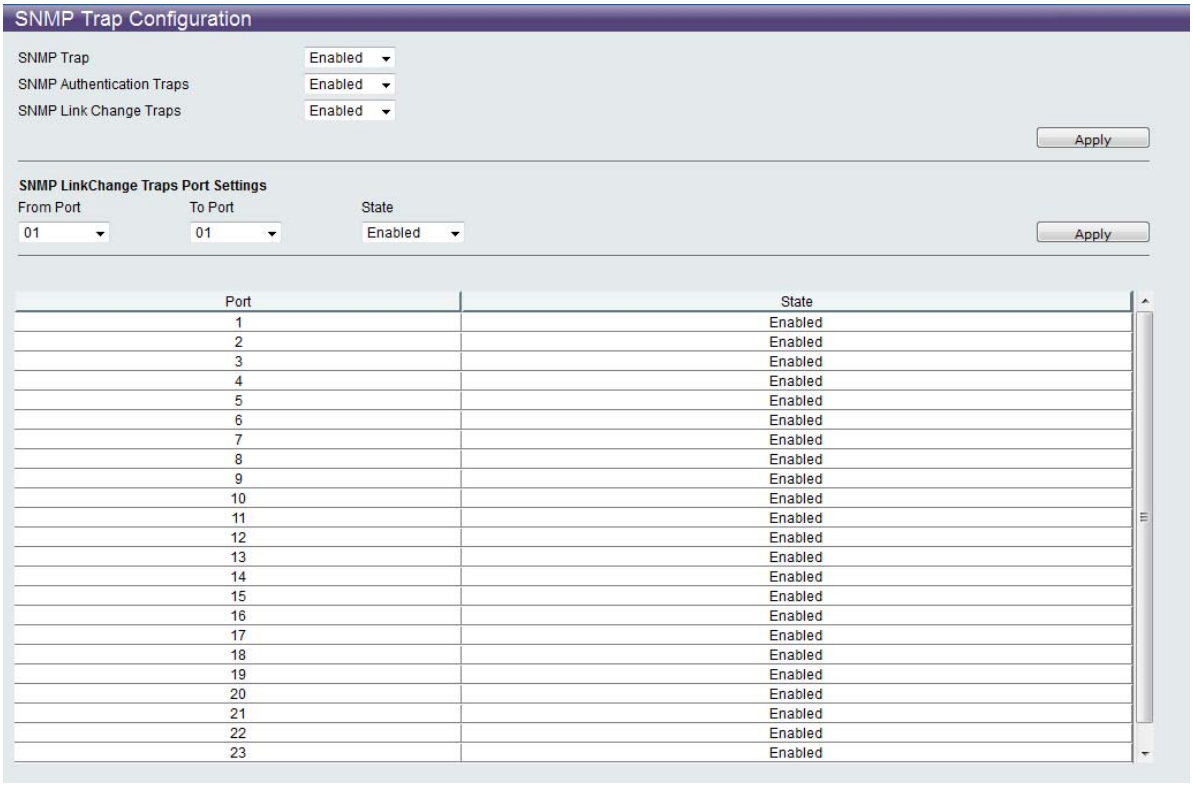
Parameter	Description
Engine ID	Specifies the SNMP Engine ID used here.

To change the Engine ID, enter the new Engine ID in the space provided and click the **Apply** button.

SNMP Trap Configuration

The following window is used to enable and disable trap settings for the SNMP function on the Switch.

To view this window for configuration, click **Configuration > SNMP Settings > SNMP Trap Configuration**:



In this window, the following parameters can be configured:

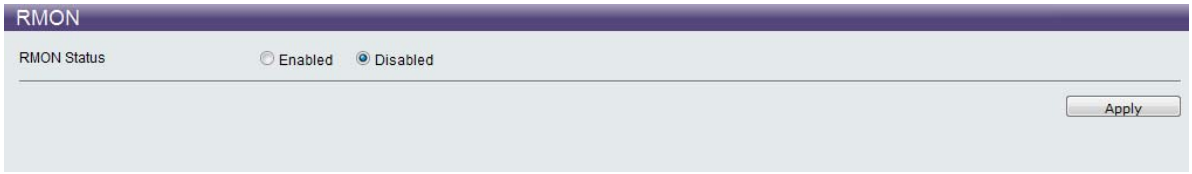
Parameter	Description
SNMP Trap	Specifies to enable or disable SNMP Traps.
SNMP Authentication Traps	Specifies to enable or disable SNMP Authentication Traps.
SNMP Link Change Traps	Specifies to enable or disable SNMP Link Change Traps.
From Port ~ To Port	Specifies the list of port used for this configuration.
State	Specifies to enable or disable the SNMP LinkChange Traps port settings state.

Click on the **Apply** button to accept the changes made.

RMON

Users can enable and disable remote monitoring (RMON) status for the SNMP function on the Switch.

To view this window for configuration, click **Configuration > SNMP Settings > RMON**:



In this window, the following parameters can be configured:

Parameter	Description
RMON Status	Specifies to enable or disable the RMON status.

Click on the **Apply** button to accept the changes made.

3 Layer 2 Features

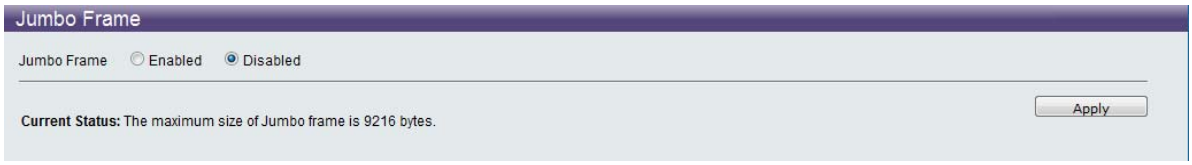
CHAPTER

The following section will aid the user in configuring Layer 2 functions for the Switch. The Switch includes various functions all discussed in detail in the following section.

Jumbo Frame

This window will enable or disable the Jumbo Frame function on the Switch. The default is Enabled. When Enabled, jumbo frames (frames larger than the standard Ethernet frame size of 1522 bytes) with a maximum size of 9216 bytes can be transmitted by the Switch.

To view this window, click **L2 Features > Jumbo Frame**:



Click on the **Apply** button to accept the changes.

VLANs

Understanding IEEE 802.1p Priority

Priority tagging is a function defined by the IEEE 802.1p standard designed to provide a means of managing traffic on a network where many different types of data may be transmitted simultaneously. It is intended to alleviate problems associated with the delivery of time critical data over congested networks. The quality of applications that are dependent on such time critical data, such as video conferencing, can be severely and adversely affected by even very small delays in transmission.

Network devices that are in compliance with the IEEE 802.1p standard have the ability to recognize the priority level of data packets. These devices can also assign a priority label or tag to packets. Compliant devices can also strip priority tags from packets. This priority tag determines the packet's degree of expeditiousness and determines the queue to which it will be assigned.

Priority tags are given values from 0 to 7 with 0 being assigned to the lowest priority data and 7 assigned to the highest. The highest priority tag 7 is generally only used for data associated with video or audio applications, which are sensitive to even slight delays, or for data from specified end users whose data transmissions warrant special consideration.

The Switch allows you to further tailor how priority tagged data packets are handled on your network. Using queues to manage priority tagged data allows you to specify its relative priority to suit the needs of your network. There may be circumstances where it would be advantageous to group two or more differently tagged packets into the same queue. Generally, however, it is recommended that the highest priority queue, Queue 7, be reserved for data packets with a priority value of 7. Packets that have not been given any priority value are placed in Queue 0 and thus given the lowest priority for delivery.

Strict mode and weighted round robin system are employed on the Switch to determine the rate at which the queues are emptied of packets. The ratio used for clearing the queues is 4:1. This means that the highest priority queue, Queue 7, will clear 4 packets for every 1 packet cleared from Queue 0.

Remember, the priority queue settings on the Switch are for all ports, and all devices connected to the Switch will be affected. This priority queuing system will be especially beneficial if your network employs switches with the capability of assigning priority tags.

VLAN Description

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLANs can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLANs also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLANs can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

Notes About VLANs

No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLANs without a network device performing a routing function between the VLANs.

The Switch supports IEEE 802.1Q VLANs and Port-Based VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.

The Switch's default is to assign all ports to a single 802.1Q VLAN named "default."

The "default" VLAN has a VID = 1.

The member ports of Port-based VLANs may overlap, if desired.

IEEE 802.1Q VLANs

Some relevant terms:

- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.

- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.
- **Ingress port** - A port on a switch where packets are flowing into the Switch and VLAN decisions must be made.
- **Egress port** - A port on a switch where packets are flowing out of the Switch, either to another switch or to an end station, and tagging decisions must be made.

IEEE 802.1Q (tagged) VLANs are implemented on the Switch. 802.1Q VLANs require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLANs allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

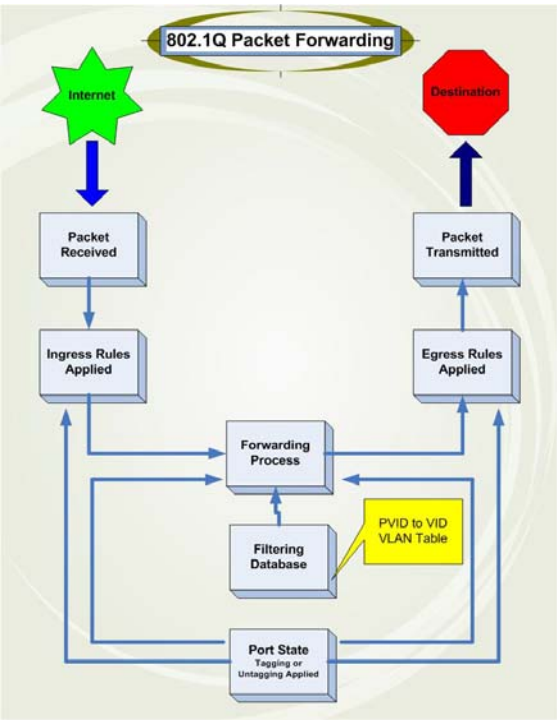
VLANs can also provide a level of security to your network. IEEE 802.1Q VLANs will only deliver packets between stations that are members of the VLAN.

Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLANs allows VLANs to work with legacy switches that don't recognize VLAN tags in packet headers. The tagging feature allows VLANs to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

The IEEE 802.1Q standard restricts the forwarding of untagged packets to the VLAN of which the receiving port is a member.

The main characteristics of IEEE 802.1Q are as follows:

- Assigns packets to VLANs by filtering.
- Assumes the presence of a single global spanning tree.
- Uses an explicit tagging scheme with one-level tagging.
- 802.1Q VLAN Packet Forwarding
- Packet forwarding decisions are made based upon the following three types of rules:
- Ingress rules - rules relevant to the classification of received frames belonging to a VLAN.
- Forwarding rules between ports - decides whether to filter or forward the packet.
- Egress rules - determines if the packet must be sent tagged or untagged.

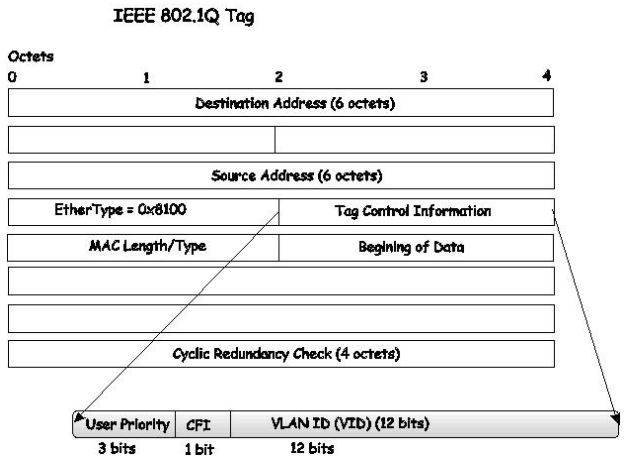


802.1Q VLAN Tags

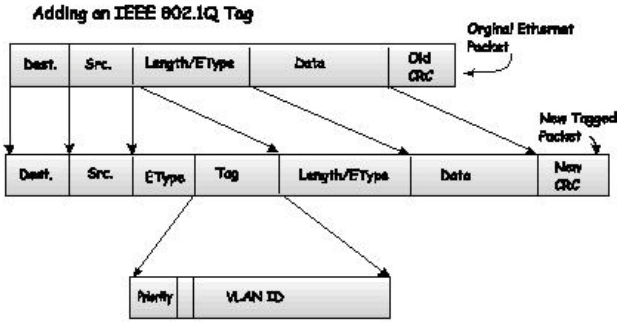
The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the EtherType field. When a packet's

EtherType field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of three bits of user priority, one bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and twelve bits of VLAN ID (VID). The three bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is twelve bits long, 4094 unique VLANs can be identified.

The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.



The EtherType and VLAN ID are inserted after the MAC source address, but before the original EtherType/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.



Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLANs to span network devices (and indeed, the entire network, if all network devices are 802.1Q compliant).

Unfortunately, not all network devices are 802.1Q compliant. These devices are referred to as tag-unaware. 802.1Q devices are referred to as tag-aware.

Prior to the adoption of 802.1Q VLANs, port-based and MAC-based VLANs were in common use. These VLANs relied upon a Port VLAN ID (PVID) to forward packets. A packet received on a given port would be assigned that port's PVID and then be forwarded to the port that corresponded to the packet's destination address (found in the Switch's forwarding table). If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the Switch will drop the packet.

Within the Switch, different PVIDs mean different VLANs (remember that two VLANs cannot communicate without an external router). So, VLAN identification based upon the PVIDs cannot create VLANs that extend outside a given switch (or switch stack).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the Switch. If no VLANs are defined on the Switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLANs are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet-forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVIDs within the Switch to VIDs on the network. The Switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VIDs are different, the Switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VIDs as the Switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted - should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Tagging and Untagging

Every port on an 802.1Q compliant switch can be configured as tagging or untagging.

Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into and out of it. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. Other 802.1Q compliant devices on the network to make packet-forwarding decisions can then use the VLAN information in the tag.

Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into and out of those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Ingress Filtering

A port on a switch where packets are flowing into the Switch and VLAN decisions must be made is referred to as an ingress port. If ingress filtering is enabled for a port, the Switch will examine the VLAN information in the packet header (if present) and decide whether or not to forward the packet.

If the packet is tagged with VLAN information, the ingress port will first determine if the ingress port itself is a member of the tagged VLAN. If it is not, the packet will be dropped. If the ingress port is a member of the 802.1Q VLAN, the Switch then determines if the destination port is a member of the 802.1Q VLAN. If it is not, the packet is dropped. If the destination port is a member of the 802.1Q VLAN, the packet is forwarded and the destination port transmits it to its attached network segment.

If the packet is not tagged with VLAN information, the ingress port will tag the packet with its own PVID as a VID (if the port is a tagging port). The switch then determines if the destination port is a member of the same VLAN (has the same VID) as the ingress port. If it does not, the packet is dropped. If it has the same VID, the packet is forwarded and the destination port transmits it on its attached network segment.

This process is referred to as ingress filtering and is used to conserve bandwidth within the Switch by dropping packets that are not on the same VLAN as the ingress port at the point of reception. This eliminates the subsequent processing of packets that will just be dropped by the destination port.

Default VLANs

The Switch initially configures one VLAN, VID = 1, called "default." The factory default setting assigns all ports on the Switch to the "default." As new VLANs are configured in Port-based mode, their respective member ports are removed from the "default."

Packets cannot cross VLANs. If a member of one VLAN wants to connect to another VLAN, the link must be through an external router.

NOTE

If no VLANs are configured on the Switch, then all packets will be forwarded to any destination port. Packets with unknown source addresses will be flooded to all ports. Broadcast and multicast packets will also be flooded to all ports.

An example is presented below:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineering	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4

Port-based VLANs

Port-based VLANs limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

On port-based VLANs, NICs do not need to be able to identify 802.1Q tags in packet headers. NICs send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another switch port, VLAN considerations come into play to decide if the packet gets dropped by the Switch or delivered.

VLAN Segmentation

Take for example a packet that is transmitted by a machine on Port 1 that is a member of VLAN 2. If the destination lies on another port (found through a normal forwarding table lookup), the Switch then looks to see if the other port (Port 10) is a member of VLAN 2 (and can therefore receive VLAN 2 packets). If Port 10 is not a member of VLAN 2, then the packet will be dropped by the Switch and will not reach its destination. If Port 10 is a member of VLAN 2, the packet will go through. This selective forwarding feature based on VLAN criteria is how VLANs segment networks. The key point being that Port 1 will only transmit on VLAN 2.

Network resources can be shared across VLANs. This is achieved by setting up overlapping VLANs. That is ports can belong to more than one VLAN group. For example, by setting VLAN 1 members to

ports 1, 2, 3 and 4 and VLAN 2 members to ports 1, 5, 6 and 7, Port 1 will belong to two VLAN groups. Ports 8, 9 and 10 are not configured to any VLAN group. This means ports 8, 9 and 10 are in the same VLAN group.

VLAN and Trunk Groups

The members of a trunk group have the same VLAN setting. Any VLAN setting on the members of a trunk group will apply to the other member ports.

NOTE

In order to use VLAN segmentation in conjunction with port trunk groups, you can first set the port trunk group(s), and then you may configure VLAN settings. If you wish to change the port trunk grouping with VLANs already in place, you will not need to reconfigure the VLAN settings after changing the port trunk group settings. VLAN settings will automatically change in conjunction with the change of the port trunk group settings.

Q-in-Q VLANs

Q-in-Q VLANs (also sometimes referred to as double VLANs) allow network providers to expand their VLAN configurations to place customer VLANs within a larger inclusive VLAN, which adds a new layer to the VLAN configuration. This basically lets large ISP's create L2 Virtual Private Networks and also create transparent LANs for their customers, which will connect two or more customer LAN points without over-complicating configurations on the client's side. Not only will over-complication be avoided, but also now the administrator has over 4000 VLANs in which over 4000 VLANs can be placed, therefore greatly expanding the VLAN network and enabling greater support of customers utilizing multiple VLANs on the network.

Q-in-Q VLANs are basically VLAN tags placed within existing IEEE 802.1Q VLANs which we will call SPVIDs (Service Provider VLAN IDs). These VLANs are marked by a TPID (Tagged Protocol ID), configured in hex form to be encapsulated within the VLAN tag of the packet. This identifies the packet as double-tagged and segregates it from other VLANs on the network, therefore creating a hierarchy of VLANs within a single packet.

Here is an example Q-in-Q VLAN tagged packet:

Destination Address	Source Address	SPVLAN (TPID + Service Provider VLAN Tag)	802.1Q CEVLAN Tag (TPID + Customer VLAN Tag)	Ether Type	Payload

Regulations for Q-in-Q VLANs

Some rules and regulations apply with the implementation of the Q-in-Q VLAN procedure.

1. All ports must be configured for the SPVID and its corresponding TPID on the Service Provider's edge switch.
2. All ports must be configured as Access Ports or Uplink ports. Access ports can only be Ethernet ports while Uplink ports must be Gigabit ports.
3. Provider Edge switches must allow frames of at least 1522 bytes or more, due to the addition of the SPVID tag.
4. Access Ports must be an un-tagged port of the service provider VLANs. Uplink Ports must be a tagged port of the service provider VLANs.
5. The switch cannot have both Q-in-Q and normal VLANs co-existing. Once the change of VLAN is made, all Access Control lists are cleared and must be reconfigured.

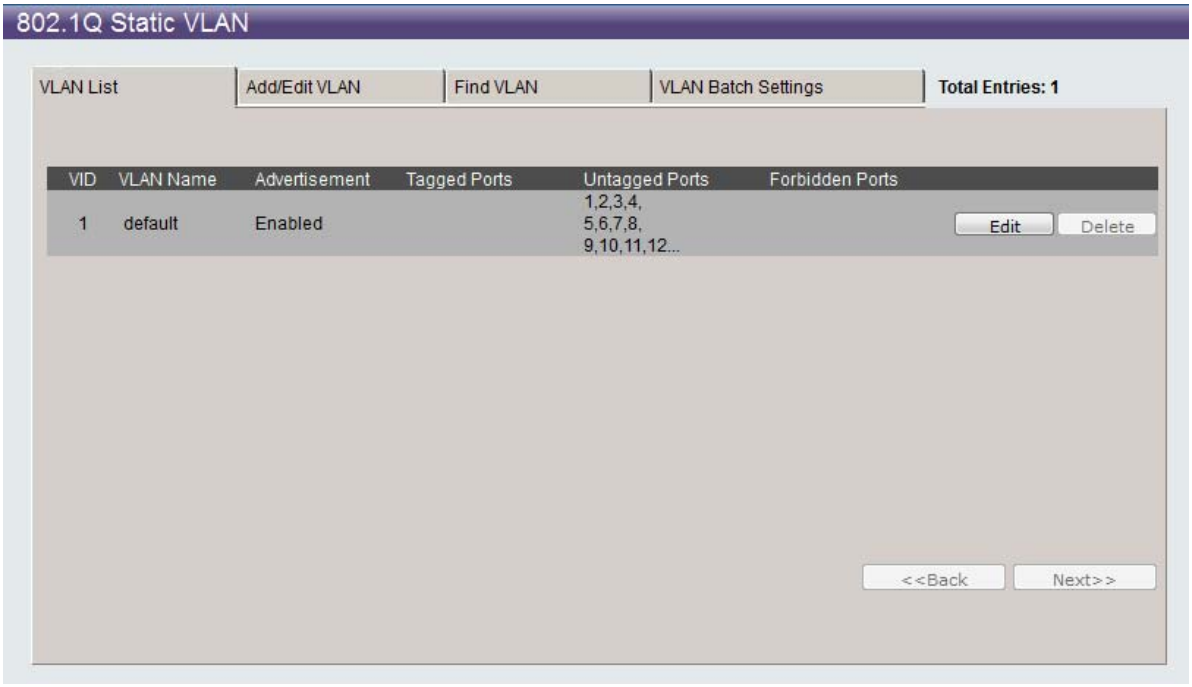
6 Before Q-in-Q VLANs are enabled, users need to disable STP and GVRP manually.

7 All packets sent from the CPU to the Access ports must be untagged.

802.1Q Static VLAN

This window lists all previously configured VLANs by VLAN ID and VLAN Name.

To view this window, click **L2 Features > 802.1Q Static VLAN**:



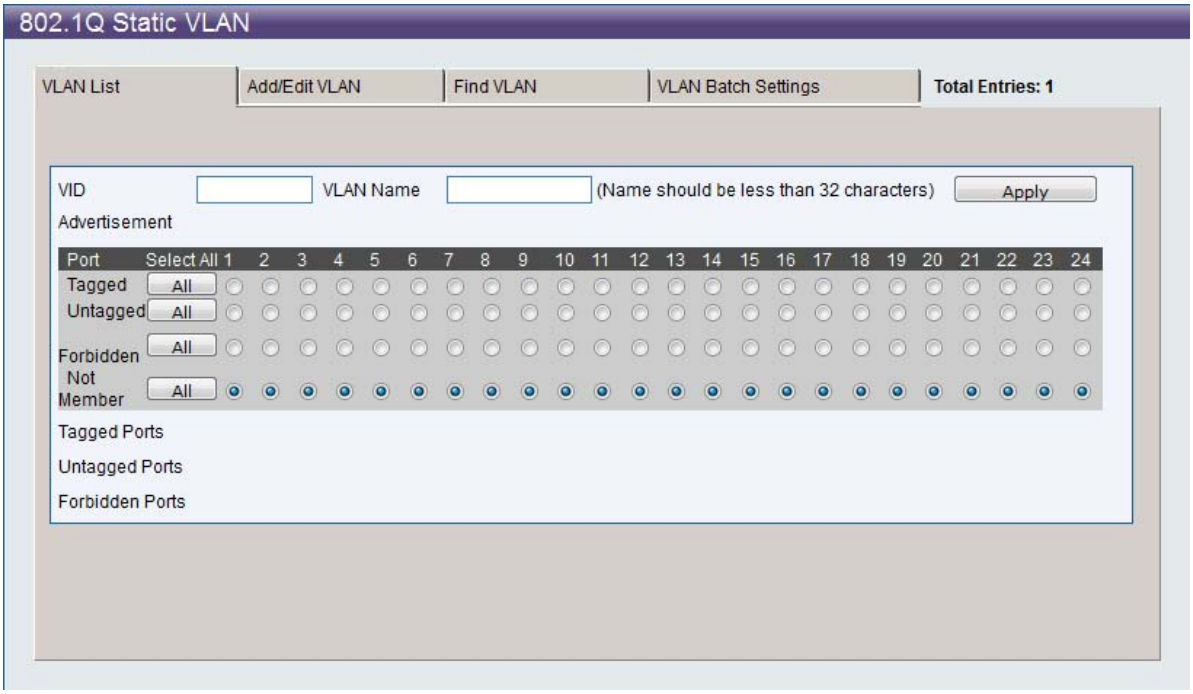
To create a new 802.1Q VLAN entry, click the **Add/Edit VLAN** tab at the top of the window. A new tab will appear, as shown in the first figure on the next page, to configure the port settings and to assign a unique name and number to the new VLAN.

To edit an existing 802.1Q VLAN entry, click the **Edit** button next to the corresponding VLAN entry above. A new tab will appear, as shown in the second figure on the next page.

See the table on the next page for a description of the parameters of the **802.1Q Static VLAN** window's **Add/Edit VLAN** tab.

NOTE

After all IP interfaces are set for configurations, VLANs on the Switch can be routed without any additional steps.



To return to the initial **802.1Q Static VLAN** window, click the **VLAN List** tab at the top of the window. To change an existing 802.1Q static VLAN entry, click the corresponding **Edit** button. A new window will appear to configure the port settings and to assign a unique name and number to the new VLAN. See the table below for a description of the parameters in the new window.

NOTE

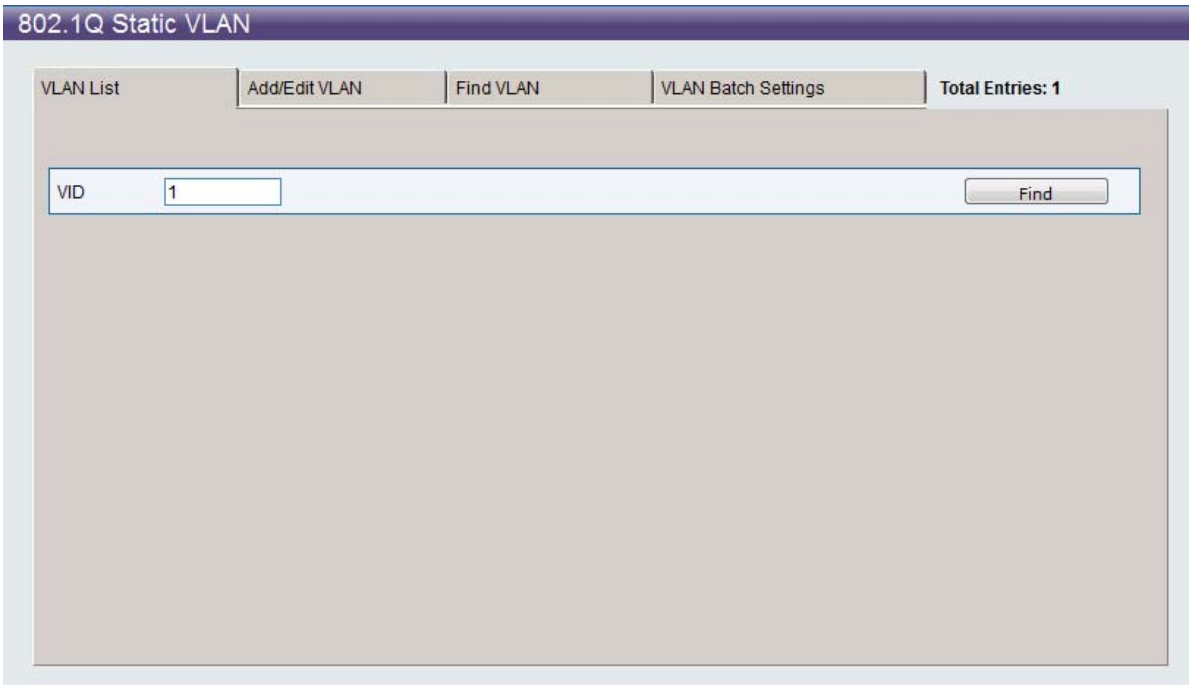
The Switch supports up to 4k static VLAN entries.

In this window, the following parameters can be configured:

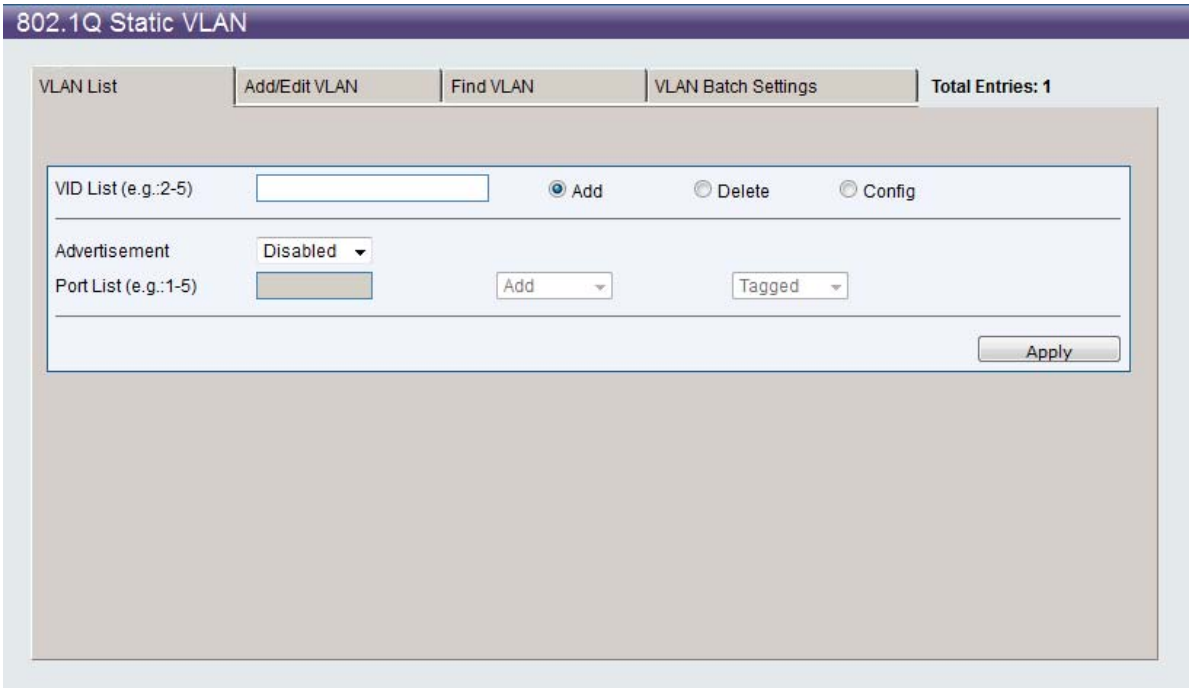
Parameter	Description
VID (VLAN ID)	Allows the entry of a VLAN ID, or displays the VLAN ID of an existing VLAN in the **Add/Edit VLAN** tab. VLANs can be identified by either the VID or the VLAN name.
VLAN Name	Allows the entry of a name for a new VLAN, or modifying the VLAN name in the **Add/Edit VLAN** tab. VLAN Name should be no more than 32 characters in length.
Advertisement	Enabling this function will allow the Switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Port Settings	Allows an individual port to be specified as member of a VLAN.
Tagged	Specifies the port as 802.1Q tagged. Checking the box will designate the port as Tagged.
Untagged	Specifies the port as 802.1Q untagged. Checking the box will designate the port as untagged.
Forbidden	Select this to specify the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically.
Not Member	Allows an individual port to be specified as a non-VLAN member.

Click on the **Apply** button to accept the changes made.

To search for a VLAN, click the **Find VLAN** tab at the top of the window (see below), enter a VLAN ID, and click **Find** to display the settings for a previously configured VLAN.



To create a VLAN Batch entry, click the **VLAN Batch Settings** tab at the top of the window, which will display the following window:



In this window, the following parameters can be configured:

Parameter	Description
VID List (e.g.: 2-5)	Enter a VLAN ID List that can be added, deleted or configured.
Advertisement	Enabling this function will allow the Switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Port List (e.g.: 1-5)	Allows an individual port list to be added or deleted as a member of the VLAN.
Tagged	Specifies the port as 802.1Q tagged. Checking the box will designate the port as Tagged.
Untagged	Specifies the port as 802.1Q untagged. Checking the box will designate the port as untagged.
Forbidden	Select this to specify the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically.

Click on the **Apply** button to accept the changes made.

Q-in-Q Folder

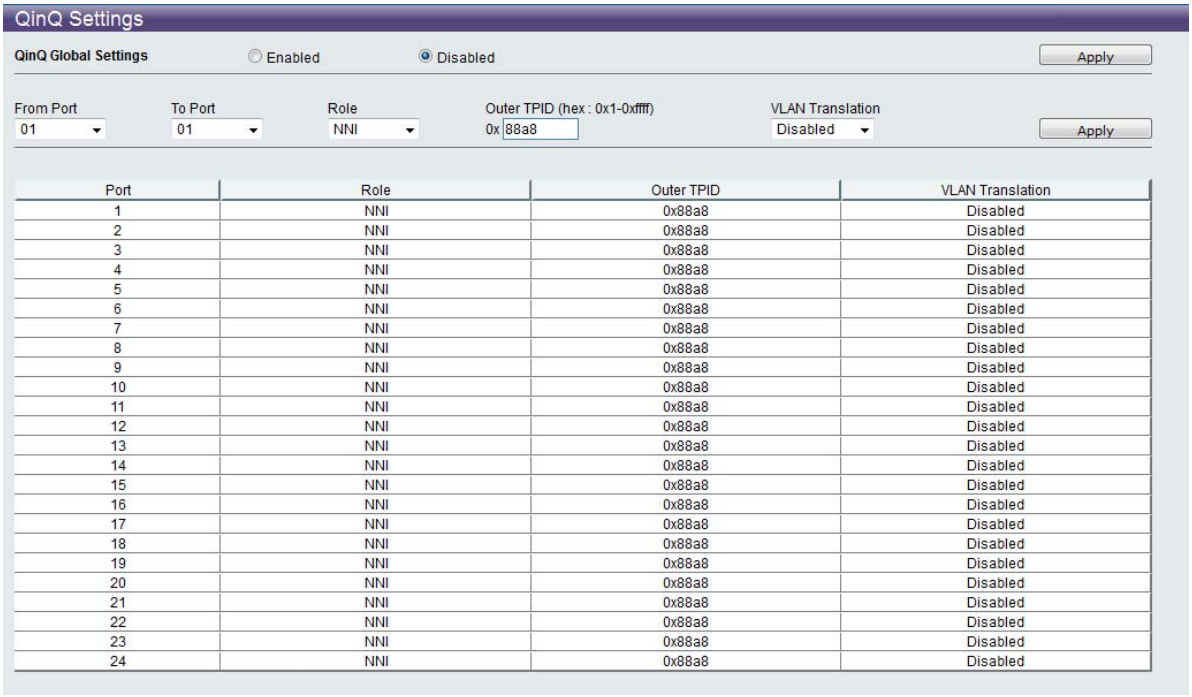
This function allows the user to enable or disable the Q-in-Q function. Q-in-Q is designed for service providers to carry traffic from multiple users across a network.

Q-in-Q is used to maintain customer specific VLAN and Layer 2 protocol configurations even when the same VLAN ID is being used by different customers. This is achieved by inserting SPVLAN tags into the customer's frames when they enter the service provider's network, and then removing the tags when the frames leave the network.

Customers of a service provider may have different or specific requirements regarding their internal VLAN IDs and the number of VLANs that can be supported. Therefore customers in the same service provider network may have VLAN ranges that overlap, which might cause traffic to become mixed up. So assigning a unique range of VLAN IDs to each customer might cause restrictions on some of their configurations requiring intense processing of VLAN mapping tables which may exceed the VLAN mapping limit. Q-in-Q uses a single service provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer's VLAN IDs are segregated within the service provider's network even when they use the same customer specific VLAN ID. Q-in-Q expands the VLAN space available while preserving the customer's original tagged packets and adding SPVLAN tags to each new frame.

Q-in-Q Settings

To view this window, click **L2 Features > Q-in-Q > Q-in-Q Settings**:



In this window, the following parameters can be configured:

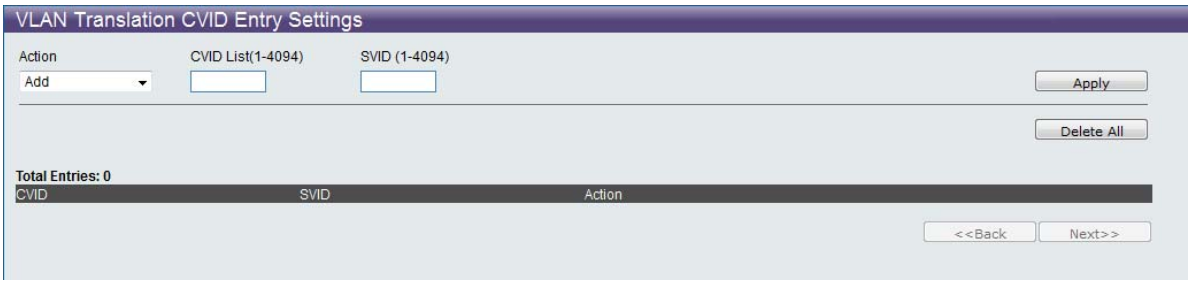
Parameter	Description
Q-in-Q Global Settings	Click the radio button to enable or disable the Q-in-Q Global Settings.
From Port/To Port	A consecutive group of ports that are part of the VLAN configuration starting with the selected port.
Role	The user can choose between UNI or NNI role. *UNI* – To select a user-network interface which specifies that communication between the specified user and a specified network will occur. *NNI* – To select a network-to-network interface specifies that communication between two specified networks will occur.
Outer TPID (hex: 0x1 -0xffff)	The Outer TPID is used for learning and switching packets. The Outer TPID constructs and inserts the outer tag into the packet based on the VLAN ID and Inner Priority.
VLAN Translation	Enable or disable VLAN Translation. This translates the VLAN IDs carried in the data packets received from private networks into those used in the Service Provider's network. The default is *Disabled*. Note: To use this function, Trust CVID must also be enabled.

Click on the **Apply** button to accept the changes made.

VLAN Translation Settings

VLAN translation translates the VLAN ID carried in the data packets it receives from private networks into those used in the Service Providers network.

To view this window click **L2 Features > Q-in-Q > VLAN Translation CVID Entry Settings**:



In this window, the following parameters can be configured:

Parameter	Description
Action	Specify to *Add* or *Replace* Service Provider VLAN ID (SVID) packets.
CVID (1-4094)	The customer VLAN ID List to which the tagged packets will be added.
SVID(1-4094)	This configures the VLAN to join the Service Providers VLAN as a tagged member.

Click on the **Apply** button to accept the changes made.

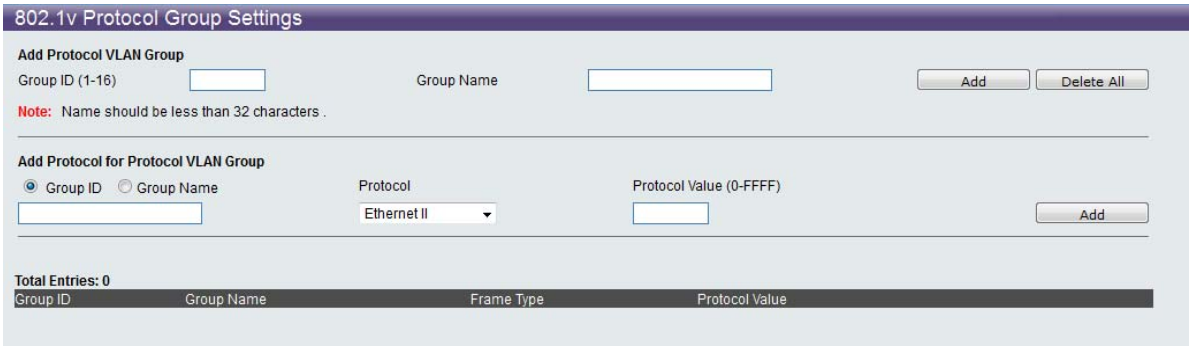
Click on the **Delete All** button to remove all the entries.

802.1v Protocol VLAN Folder

The window allows the user to create Protocol VLAN groups and add protocols to that group. The 802.1v Protocol VLAN Group Settings supports multiple VLANs for each protocol and allows the user to configure the untagged ports of different protocols on the same physical port. For example it allows the user to configure an 802.1Q and 802.1v untagged port on the same physical port. The lower half of the window displays any previously created groups.

802.1v Protocol Group Settings

To view this window, click **L2 Features > 802.1v Protocol VLAN > 802.1v Protocol Group Settings:**



In this window, the following parameters can be configured:

Parameter	Description
Group ID (1-16)	Select an ID number for the group, between *1* and *16*.
Group Name	This is used to identify the new Protocol VLAN group. Type an alphanumeric string of up to 32 characters.
Protocol	This function maps packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it. Use the drop-down menu to toggle between *Ethernet II* and *IEEE802.3 SNAP*.
Protocol Value (0-FFFF)	Enter a value for the Group.

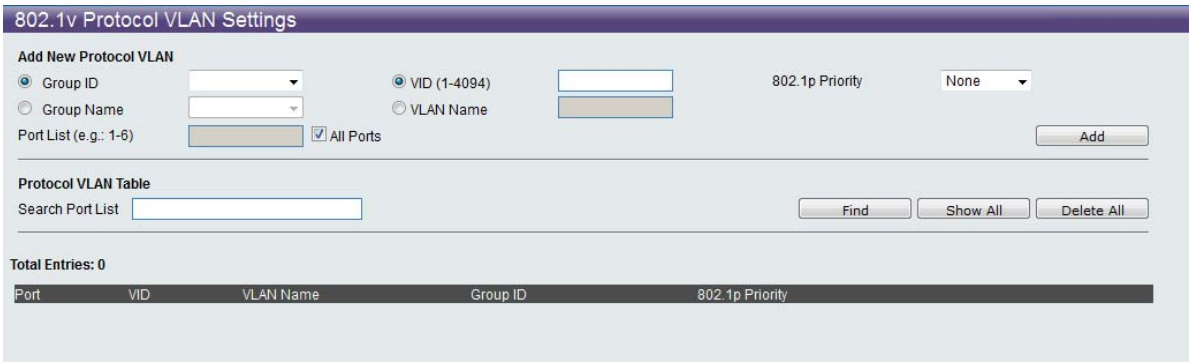
Click on the **Add** button to add a new entry.

Click on the **Delete All** button to remove all the entries.

802.1v Protocol VLAN Settings

The window allows the user to configure Protocol VLAN settings. The lower half of the window displays any previously created settings.

To view this window, click **L2 Features > 802.1v Protocol VLAN > 802.1v Protocol VLAN Settings:**



In this window, the following parameters can be configured:

Parameter	Description
Group ID	Click the corresponding radio button to select a previously configured Group ID from the drop-down menu.
Group Name	Click the corresponding radio button to select a previously configured Group Name from the drop-down menu.
VID (1-4094)	Click the radio button to enter the VID. This is the VLAN ID that, along with the VLAN Name, identifies the VLAN the user wishes to create.
VLAN Name	Click the radio button to enter a VLAN Name. This is the VLAN Name that, along with the VLAN ID, identifies the VLAN the user wishes to create.
802.1p Priority	This parameter is specified to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Port List (e.g.: 1-6)	Here the user is only allowed to apply this feature to all the ports. The **All Ports** option will be ticked.
Search Port List	This function allows the user to search all previously configured port list settings and display them on the lower half of the table. To search for a port list enter the port number you wish to view and click **Find**. To display all previously configured port lists on the bottom half of the window click the **Show All** button, to clear all previously configured lists click the **Delete All** button.

Click on the **Add** button to add a new entry.

Click on the **Find** button to find a specific entry based on the parameters entered.

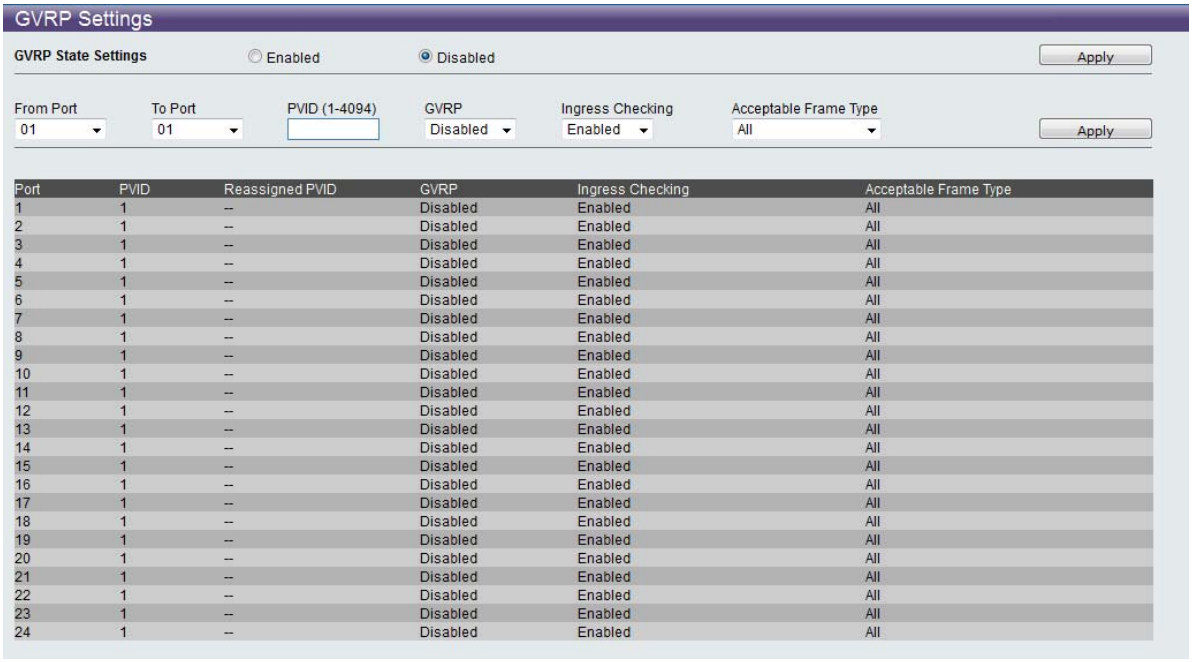
Click on the **Show All** button to view all the existing entries.

Click on the **Delete All** button to remove all the entries.

GVRP Settings

This window allows the user to determine whether the Switch will share its VLAN configuration information with other GARP VLAN Registration Protocol (GVRP) enabled switches. In addition, Ingress Checking can be used to limit traffic by filtering incoming packets whose PVID do not match the PVID of the port. Results can be seen in the table under the configuration settings, as seen below.

To view this window, click **L2 Features > GVRP Settings**:


GVRP Settings
GVRP State Settings
Enabled
Disabled
Apply
From Port
To Port
PVID (1-4094)
GVRP
Ingress Checking
Acceptable Frame Type
01
01
Disabled
Enabled
All
Apply
Port PVID Reassigned PVID GVRP Ingress Checking Acceptable Frame Type
1 1 -- Disabled Enabled All
2 1 -- Disabled Enabled All
3 1 -- Disabled Enabled All
4 1 -- Disabled Enabled All
5 1 -- Disabled Enabled All
6 1 -- Disabled Enabled All
7 1 -- Disabled Enabled All
8 1 -- Disabled Enabled All
9 1 -- Disabled Enabled All
10 1 -- Disabled Enabled All
11 1 -- Disabled Enabled All
12 1 -- Disabled Enabled All
13 1 -- Disabled Enabled All
14 1 -- Disabled Enabled All
15 1 -- Disabled Enabled All
16 1 -- Disabled Enabled All
17 1 -- Disabled Enabled All
18 1 -- Disabled Enabled All
19 1 -- Disabled Enabled All
20 1 -- Disabled Enabled All
21 1 -- Disabled Enabled All
22 1 -- Disabled Enabled All
23 1 -- Disabled Enabled All
24 1 -- Disabled Enabled All

In this window, the following parameters can be configured:

Parameter	Description
GVRP State Settings	Click the radio buttons to enable or disable the GVRP global state settings.
From Port/To Port	These two fields allow you to specify the range of ports that will be included in the Port-based VLAN that you are creating using the **802.1Q Port Settings** window.
PVID (1-4094)	Enter a PVID assignment for each port, which may be manually assigned to a VLAN when created in the 802.1Q Port Settings table. The Switch's default is to assign all ports to the default VLAN with a VID of 1. The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified to accept only tagged frames - as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If the port receives a packet, and Ingress filtering is enabled, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.
GVRP	The Group VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is *Disabled* by default.

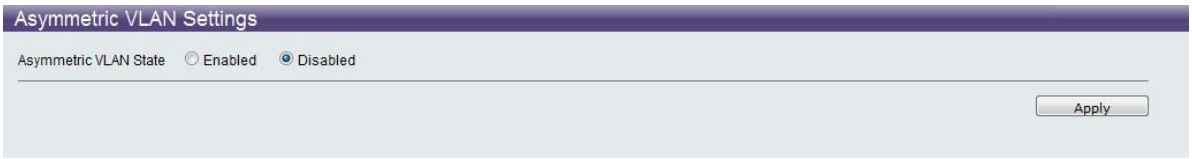
Parameter	Description
Ingress Checking	This field can be toggled using the space bar between *Enabled* and *Disabled*. *Enabled* enables the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet. *Disabled* disables ingress filtering. Ingress Checking is *Enabled* by default.
Acceptable Frame Type	This field denotes the type of frame that will be accepted by the port. The user may choose between *Tagged Only*, which means only VLAN tagged frames will be accepted, and *All*, which mean both tagged and untagged frames will be accepted. *All* is enabled by default.

Click on the **Apply** button to accept the changes made.

Asymmetric VLAN Settings

Shared VLAN Learning is a primary example of the requirement for Asymmetric VLANs. Under normal circumstances, a pair of devices communicating in a VLAN environment will both send and receive using the same VLAN; however, there are some circumstances in which it is convenient to make use of two distinct VLANs, one used for A to transmit to B and the other used for B to transmit to A in these cases Asymmetric VLANs are needed. An example of when this type of configuration might be required would be if the client was on a distinct IP subnet, or if there was some confidentiality-related need to segregate traffic between the clients.

To view this window, click **L2 Features > Asymmetric VLAN Settings**:



In this window, the following parameters can be configured:

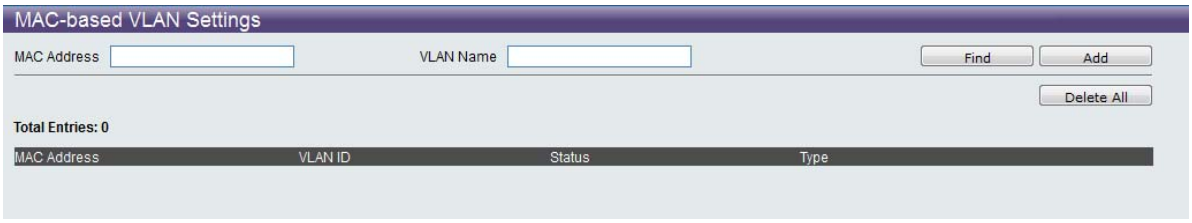
Parameter	Description
Assymetric VLAN State	Specifies to enable or disable the asymmetric VLAN settings state.

Click on the **Apply** button to accept the changes made.

MAC-based VLAN Settings

This window is used to create MAC-based VLAN entries on the switch. A MAC Address can be mapped to any existing static VLAN and multiple MAC addresses can be mapped to the same VLAN. When a static MAC-based VLAN entry is created for a user, the traffic from this user is able to be serviced under the specified VLAN. Therefore each entry specifies a relationship of a source MAC address with a VLAN.

To view this window, click **L2 Features > MAC-based VLAN Settings:**



In this window, the following parameters can be configured:

Parameter	Description
MAC Address	Specify the MAC address to be mapped.
VLAN Name	Enter the VLAN name of a previously configured VLAN.

Click on the **Find** button to find a specific entry based on the parameters entered.

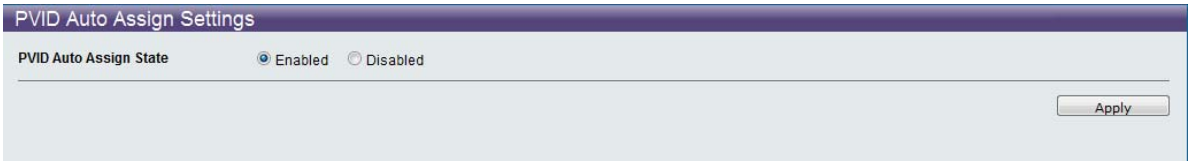
Click on the **Add** button to add a new entry.

Click on the **Delete All** button to remove all the entries.

PVID Auto Assign Settings

This enables or disables PVID Auto Assign on the Switch. PVID is the VLAN that the switch will use for forwarding and filtering purposes. If PVID Auto-Assign is *Enabled*, PVID will be possibly changed by previously set PVID or VLAN configurations. When a user configures a port to VLAN X's untagged membership, this port's PVID will be updated with VLAN X. In the form of a VLAN list command, PVID is updated with the last item on the VLAN list. When a user removes a port from the untagged membership of the PVID's VLAN, the port's PVID will be assigned to a default VLAN. When PVID Auto Assign is *Disabled*, PVID can only be changed by PVID configuration (user changes explicitly). The VLAN configuration will not automatically change the PVID. The default setting is *Enabled*.

To view this window, click **L2 Features > PVID Auto Assign Settings:**



In this window, the following parameters can be configured:

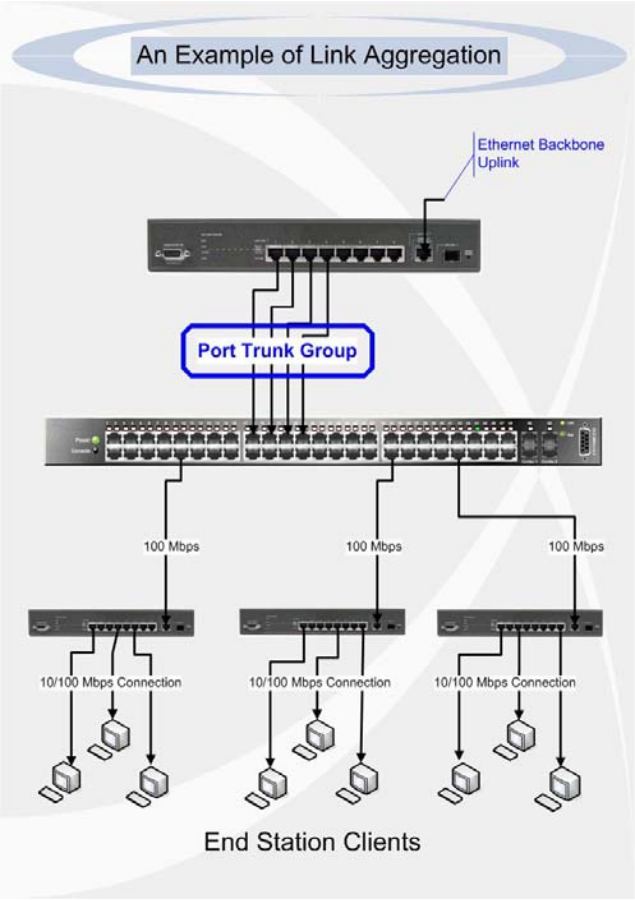
Parameter	Description
PVID Auto Assign State	Specifies to enable or disable the PVID auto assign settings state.

Click on the **Apply** button to accept the changes made.

Port Trunking

Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline. The Switch supports up to eight port trunk groups with two to eight ports in each group.



The Switch treats all ports in a trunk group as a single port. Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent.

NOTE

If any ports within the trunk group become disconnected, packets intended for the disconnected port will be load shared among the other linked ports of the link aggregation group.

Link aggregation allows several ports to be grouped together and to act as a single link. This gives a bandwidth that is a multiple of a single link's bandwidth.

Link aggregation is most commonly used to link a bandwidth intensive network device or devices, such as a server, to the backbone of a network.

The Switch allows the creation of up to eight link aggregation groups, each group consisting of two to eight links (ports). All of the ports in the group must be members of the same VLAN, and their STP

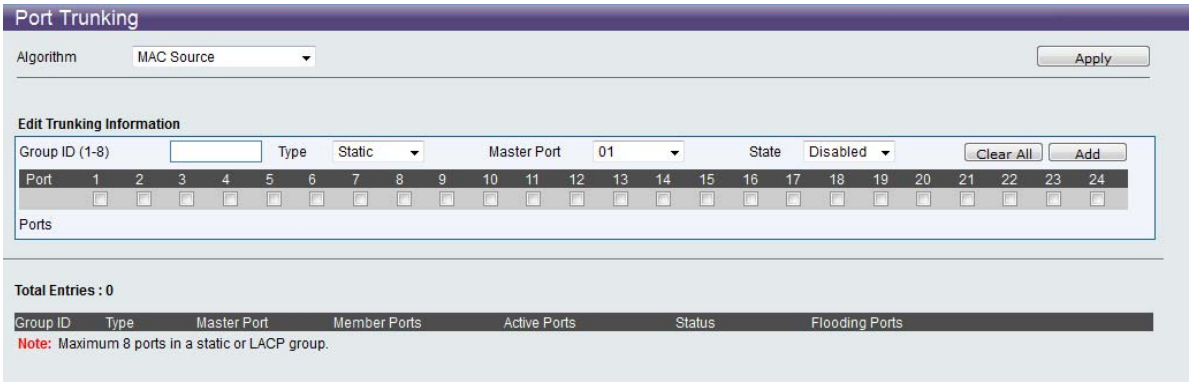
status, static multicast, traffic control; traffic segmentation and 802.1p default priority configurations must be identical. Port locking, port mirroring and 802.1X must not be enabled on the trunk group. Further, the aggregated links must all be of the same speed and should be configured as full duplex.

The Master Port of the group is to be configured by the user, and all configuration options, including the VLAN configuration that can be applied to the Master Port, are applied to the entire link aggregation group.

Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

The Spanning Tree Protocol will treat a link aggregation group as a single link, on the switch level. On the port level, the STP will use the port parameters of the Master Port in the calculation of port cost and in determining the state of the link aggregation group. If two redundant link aggregation groups are configured on the Switch, STP will block one entire group; in the same way STP will block a single port that has a redundant link.

To view this window, click **L2 Features > Port Trunking**:



In this window, the following parameters can be configured:

Parameter	Description
Algorithm	The algorithm that the Switch uses to balance the load across the ports that make up the port trunk group is defined by this definition. Choose *MAC Source*, *MAC Destination*, *MAC Source Dest*, *IP Source*, *IP Destination* or *IP Source Dest* (See the Link Aggregation section of this manual).
Group ID	Select an ID number for the group, between *1* and *8*.
Type	This pull-down menu allows you to select between *Static* and *LACP* (Link Aggregation Control Protocol). *LACP* allows for the automatic detection of links in a Port Trunking Group.
Master Port	Choose the Master Port for the trunk group using the pull-down menu.
State	Trunk groups can be toggled between *Enabled* and *Disabled*. This is used to turn a port trunking group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup aggregation group that is not under automatic control.
Active Ports	Shows the ports that are currently forwarding packets.
(Member) Ports	Choose the members of a trunked group. Up to eight ports per group can be assigned to a group.

Parameter	Description
Flooding Ports	These ports are designated for flooding broadcast, multicast, and DLF (unicast Destination Lookup Fail) packets from the CPU in a trunk group. The port is defined by software and doesn't actually exist in the hardware.

Click on the **Apply** button to accept the changes made.

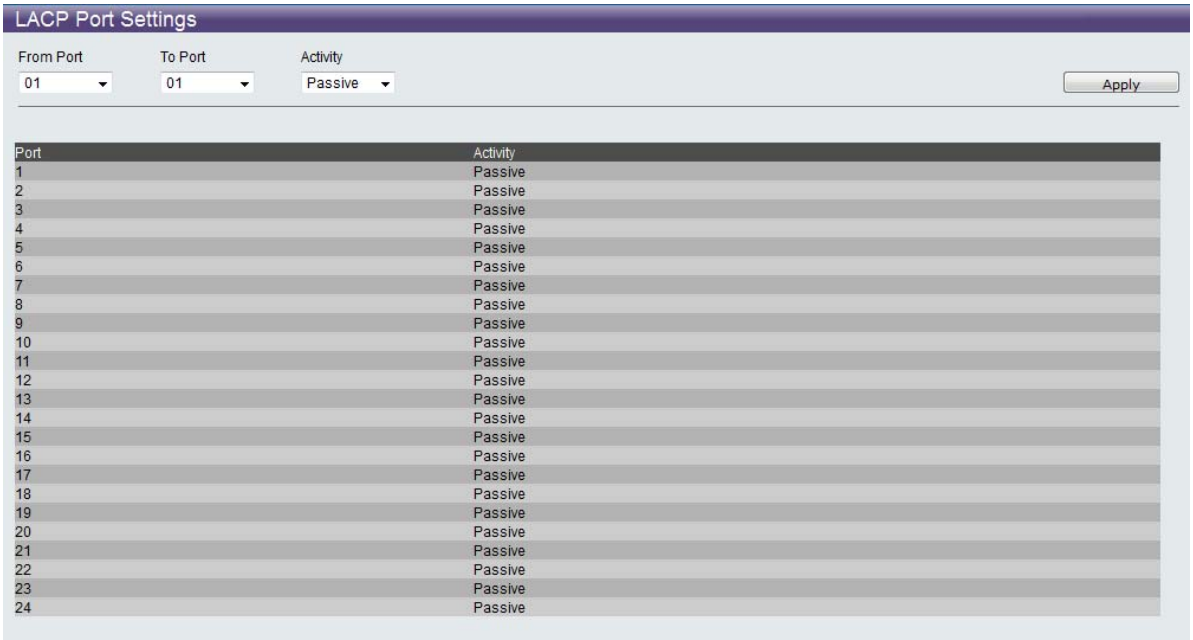
Click on the **Clear All** button to clear all the entered data from the fields.

Click on the **Add** button to add a new entry.

LACP Port Settings

This window is used to create port trunking groups on the Switch for LACP type. The user may set which ports will be active and passive in processing and sending LACP control frames.

To view this window, click **L2 Features > LACP Port Settings**:



In this window, the following parameters can be configured:

Parameter	Description
From Port/To Port	A consecutive group of ports may be configured starting with the selected port.

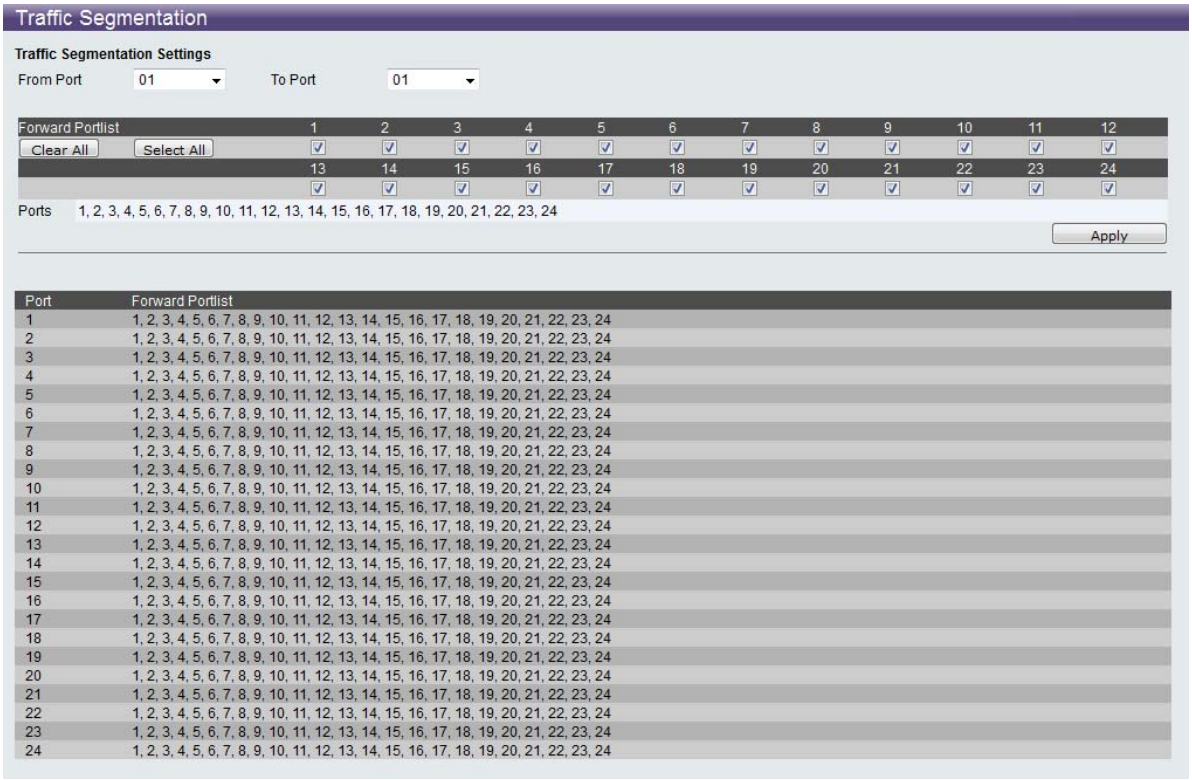
Parameter	Description
Activity	*Active* - Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP. *Passive* - LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have "active" LACP ports (see above).

Click on the **Apply** button to accept the changes made.

Traffic Segmentation

Traffic segmentation is used to limit traffic flow from a single port to a group of ports on the Switch. This method of segmenting the flow of traffic is similar to using VLANs to limit traffic, but is more restrictive. It provides a method of directing traffic that does not increase the overhead of the Switch CPU. This window allows the user to view which ports on the Switch are allowed to forward packets to other ports on the Switch. To configure new forwarding ports for a particular port, select a port from the From Port and To Port drop-down menus and click **Apply**.

To view this window, click **L2 Features > Traffic Segmentation**:



In this window, the following parameters can be configured:

Parameter	Description
From Port/To Port	Check the corresponding boxes for the port(s) to transmit packets.
Forward Portlist	Check the boxes to select which of the ports on the Switch will be able to forward packets. These ports will be allowed to receive packets from the port specified above.

Click on the **Clear All** button to clear all the entered data from the fields.

Click on the **Select All** button to select all the options for configuration.

Click on the **Apply** button to accept the changes made.

IGMP Snooping Folder

Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host. When enabled for IGMP snooping, the Switch can add or remove a port to a specific device based on IGMP messages passing through the Switch.

In order to use IGMP Snooping, it must first be enabled for the entire Switch. Then, fine-tune the settings for each VLAN using the **IGMP Snooping** windows in the **L2 Features** folder. When enabled for IGMP snooping, the Switch can open or close a port to a specific multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa. The Switch monitors IGMP messages and discontinues forwarding multicast packets when there are no longer hosts requesting that they continue.

IGMP Snooping Settings

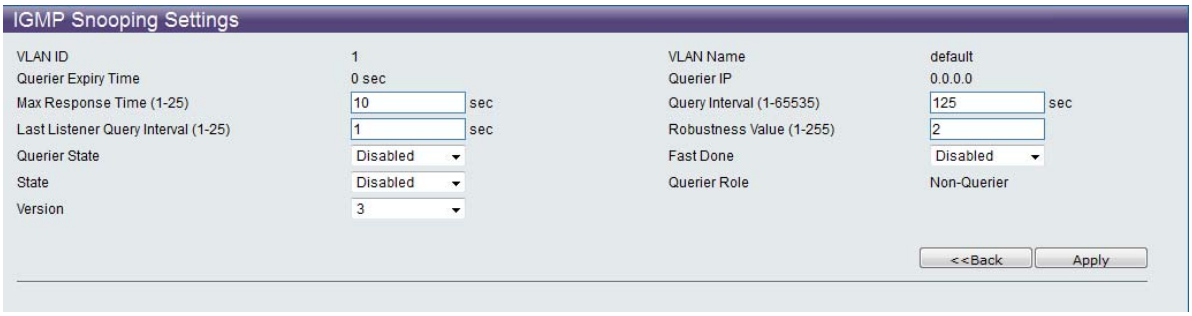
Use this window to enable or disable IGMP snooping on the Switch. The IGMP Snooping State under IGMP Snooping Global Settings can be enabled or disabled. Click **Apply** to modify the settings.

To view this window, click **L2 Features > IGMP Snooping > IGMP Snooping Settings:**

Click on the **Apply** button to accept the changes made.

Click on the **Edit** button to re-configure a specific entry.

After clicking on the **Edit** button, the following window will appear:



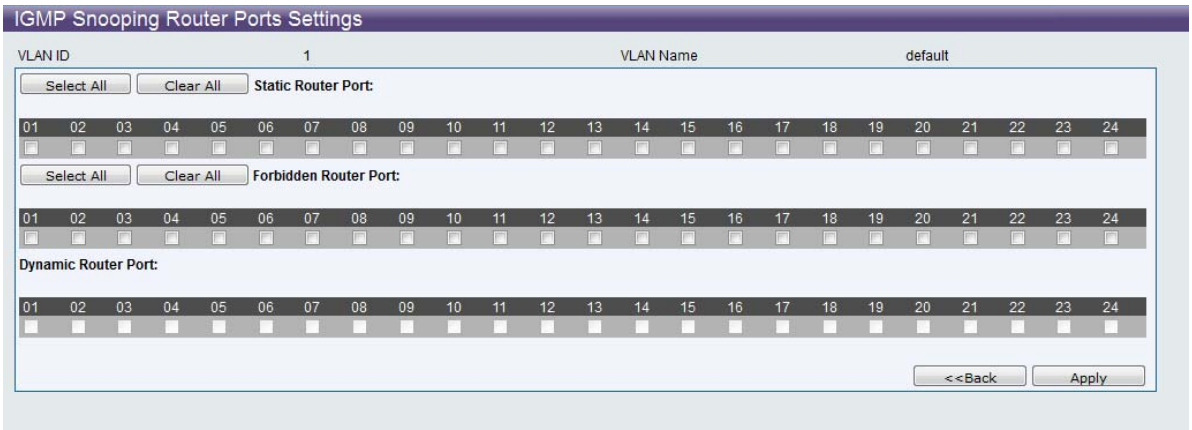
In this window, the following parameters can be configured:

Parameter	Description
VLAN ID	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN for which the user wishes to modify the IGMP Snooping Settings.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN for which the user wishes to modify the IGMP Snooping Settings.
Querier Expiry Time	Displays the querier expiry time.
Querier IP	The IP address of the device which acts as the IGMP querier for the network.
Max Response Time (1-25)	This determines the maximum amount of time in seconds to wait for reports from members. The Max Response Time field allows an entry between *1* and *25* (seconds). The default is *10*.
Query Interval (1-65535)	The Query Interval field is used to set the time (in seconds) between transmitting IGMP queries. Entries between *1* and *65535* seconds are allowed. The default is *125*.
Last Listener Query Interval (1-25)	This field specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. The default is *1*.
Robustness Value (1-255)	Adjust this variable according to expected packet loss. If packet loss on the VLAN is expected to be high, the Robustness Variable should be increased to accommodate increased packet loss. This entry field allows an entry of *1* to *255*. The default is *2*.
Querier State	Choose *Enabled* to enable transmitting IGMP query packets or *Disabled* to disable the transmitting of IGMP query packets. The default is *Disabled*.
Fast Done	This parameter allows the user to enable the Fast Leave function. Enabled, this function will allow members of a multicast group to leave the group immediately (without the implementation of the Last Member Query Timer) when an IGMP Leave Report Packet is received by the Switch. The default is *Disabled*.
State	Select *Enabled* to implement IGMP Snooping. This field is *Disabled* by default.
Querier Role	This read-only field describes the behavior of the Switch for sending query packets. Querier will denote that the Switch is sending out IGMP query packets. Non-Querier will denote that the Switch is not sending out IGMP query packets. This field will only read Querier when the Querier State and the State fields have been *Enabled*.
Version	Allows the user to configure the IGMP version used on the Switch. The default value is *3*.

Click on the **<<Back** button to return to the previous window.

Click on the **Apply** button to accept the changes made.

After clicking on the Modify Router Port link, the following window will appear:


IGMP Snooping Router Ports Settings
VLAN ID
1
VLAN Name
default
Select All
Clear All
Static Router Port:
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Select All
Clear All
Forbidden Router Port:
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Dynamic Router Port:
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
<<Back
Apply

Click on the **Select All** button to select all the options for configuration.

Click on the **Clear All** button to clear all the entered data from the fields.

Click on the **Apply** button to accept the changes made.

Click on the **<<Back** button to return to the previous window.

MLD Snooping Settings

Multicast Listener Discovery (MLD) Snooping is an IPv6 function used similarly to IGMP snooping in IPv4. It is used to discover ports on a VLAN that are requesting multicast data. Instead of flooding all ports on a selected VLAN with multicast traffic, MLD snooping will only forward multicast data to ports that wish to receive this data through the use of queries and reports produced by the requesting ports and the source of the multicast traffic.

MLD snooping is accomplished through the examination of the layer 3 part of an MLD control packet transferred between end nodes and a MLD router. When the Switch discovers that this route is requesting multicast traffic, it adds the port directly attached to it into the correct IPv6 multicast table, and begins the process of forwarding multicast traffic to that port. This entry in the multicast routing table records the port, the VLAN ID and the associated multicast IPv6 multicast group address and then considers this port to be a active listening port. The active listening ports are the only ones to receive multicast group data.

The Switch supports both MLD Snooping version 1 and MLD version 2.

MLD Control Messages

If implementing MLD snooping version 1, three types of messages are transferred between devices. These three messages are all defined by three ICMPv6 packet headers, labeled 130, 131, and 132.

1 **Multicast Listener Query, Version 1** – Similar to the IGMPv2 Host Membership Query for IPv4, and labeled as 130 in the ICMPv6 packet header, this message is sent by the router to ask if any link is

requesting multicast data. There are two types of MLD query messages emitted by the router. The General Query is used to advertise all multicast addresses that are ready to send multicast data to all listening ports, and the Multicast Specific query, which advertises a specific multicast address that is also ready. These two types of messages are distinguished by a multicast destination address located in the IPv6 header and a multicast address in the Multicast Listener Query Message.

2 **Multicast Listener Report, Version 1** – Comparable to the Host Membership Report in IGMPv2, and labeled as 131 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.

3 **Multicast Listener Done** – Akin to the Leave Group Message in IGMPv2, and labeled as 132 in the ICMPv6 packet header, this message is sent by the multicast listening port stating that it is no longer interested in receiving multicast data from a specific multicast group address, therefore stating that it is "done" with the multicast data from this address. Once this message is received by the Switch, it will no longer forward multicast traffic from a specific multicast group address to this listening port.

If implementing MLD snooping version 2, two types of messages are transferred between devices. The two messages are defined by two ICMPv6 packet headers, labeled 130 and 143.

4 **Multicast Listener Query, Version 2** – Similar to the IGMPv3 Membership Query for IPv4, and labeled as 130 in the ICMPv6 packet header, this message is sent by the router to ask if any link is requesting multicast data. With MLD snooping version 2, there are three types of MLD query messages emitted by the router, as described below:

   a The router sends a General Query message to learn which multicast addresses have listeners on an attached link. In a General Query, both the Multicast Address field and the Number of Sources field are set to zero.

   b The router sends a Multicast Address Specific Query message to learn if a particular multicast address has any listeners on an attached link. In a Multicast Address Specific Query, the Multicast Address field contains the multicast address that the router is interested in, while the Number of Sources field is set to zero.

   c The router sends a Multicast Address and Source Specific Query to learn if any of the sources from the specified list for the particular multicast address has any listeners on an attached link or not. In a Multicast Address and Source Specific Query the Multicast Address field contains the multicast address that the router is interested in, while the Source Address field(s) contain(s) the source address(es) that the router is interested in.

5 **Multicast Listener Report, Version 2** - Comparable to the Host Membership Report in IGMPv3, and labeled as 143 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.

This window is used to enable MLD Snooping on the Switch and to configure the settings for MLD snooping. To enable the MLD Snooping State, click the Enable radio button under MLD Snooping Global Settings and click **Apply**.

To view this window, click **L2 Features > MLD Snooping Settings**:

In this window, the following parameters can be configured:

Parameter	Description
MLD Snooping State	Specifies to enable or disable the MLD Snooping Global Settings state.

Click on the **Apply** button to accept the changes made.

Click on the **Edit** button to re-configure a specific entry.

After clicking on the **Edit** button, the following window will appear:

In this window, the following parameters can be configured:

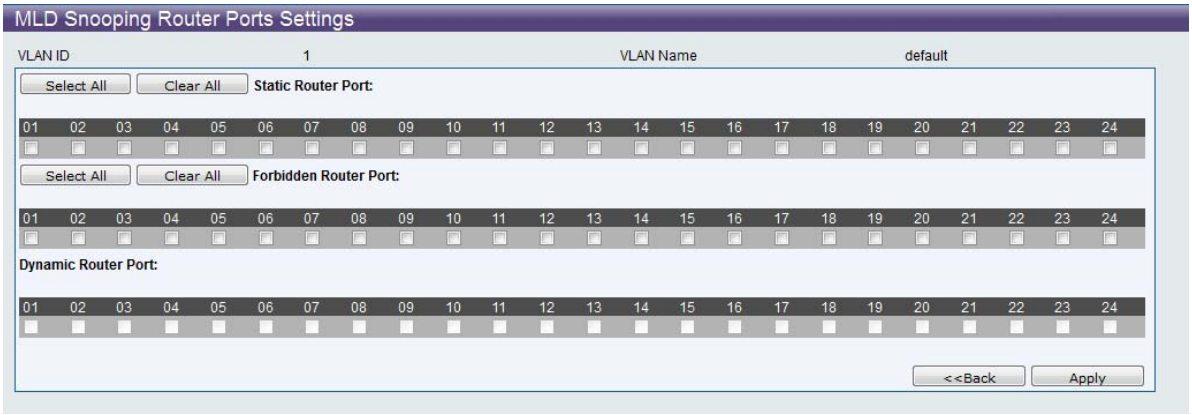
Parameter	Description
VLAN ID	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN for which the user wishes to modify the MLD Snooping Settings.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN for which the user wishes to modify the MLD Snooping Settings.
Query Interval (1-65535)	The Query Interval field is used to set the time (in seconds) between transmitting MLD queries. Entries between *1* and *65535* seconds are allowed. The default is *125*.
Max Response Time (1-25)	This determines the maximum amount of time in seconds to wait for reports from members. The Max Response Time field allows an entry between 1 and 25 (seconds). The default is *10*.
Robustness Value (1-255)	Adjust this variable according to expected packet loss. If packet loss on the VLAN is expected to be high, the Robustness Variable should be increased to accommodate increased packet loss. This entry field allows an entry of *1* to *255*. The default is *2*.
Last Listener Query Interval (1-25)	This field specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. The default is *1*.

Parameter	Description
Fast Done	This parameter allows the user to enable the Fast Leave function. *Enabled*, this function will allow members of a multicast group to leave the group immediately (without the implementation of the Last Listener Query Interval) when an MLD Leave Report Packet is received by the Switch. The default is *Disabled*.
State	Select *Enabled* to implement MLD Snooping. This field is *Disabled* by default.
Version	The read-only field displays the MLD version used on the Switch, 2.
Querier Role	This read-only field describes the behavior of the Switch for sending query packets. Querier will denote that the Switch is sending out MLD query packets. Non-Querier will denote that the Switch is not sending out MLD query packets.

Click on the **Apply** button to accept the changes made.

Click on the **<<Back** button to return to the previous window.

After clicking on the Modify Router Port link, the following window will appear:


MLD Snooping Router Ports Settings
VLAN ID
1
VLAN Name
default
Select All
Clear All
Static Router Port:
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Select All
Clear All
Forbidden Router Port:
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Dynamic Router Port:
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
<<Back
Apply

Select the desired router ports and then click **Apply** to implement any changes made.

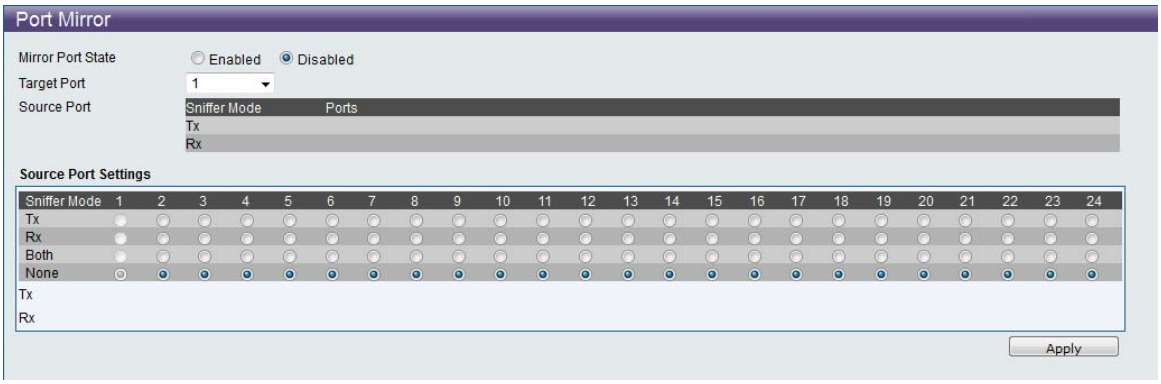
To select either all of the static router ports or all of the forbidden router ports, click the corresponding **Select All** button.

To clear either all of the selected static router ports or all of the selected forbidden router ports, click the corresponding **Clear All** button. Click **<<Back** to return to the **MLD Snooping Settings** window.

Port Mirror

The Switch allows you to copy frames transmitted and received on a port and redirect the copies to another port. You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes.

To view this window, click **Layer 2 Features > Port Mirror**:



To configure a mirror port:

1 Change the status to Enabled.

2 Select the Target Port, which receives the copies from the source port.

3 Select the Source Port from where the frames come from.

4 Click **Apply** to let the changes take effect.

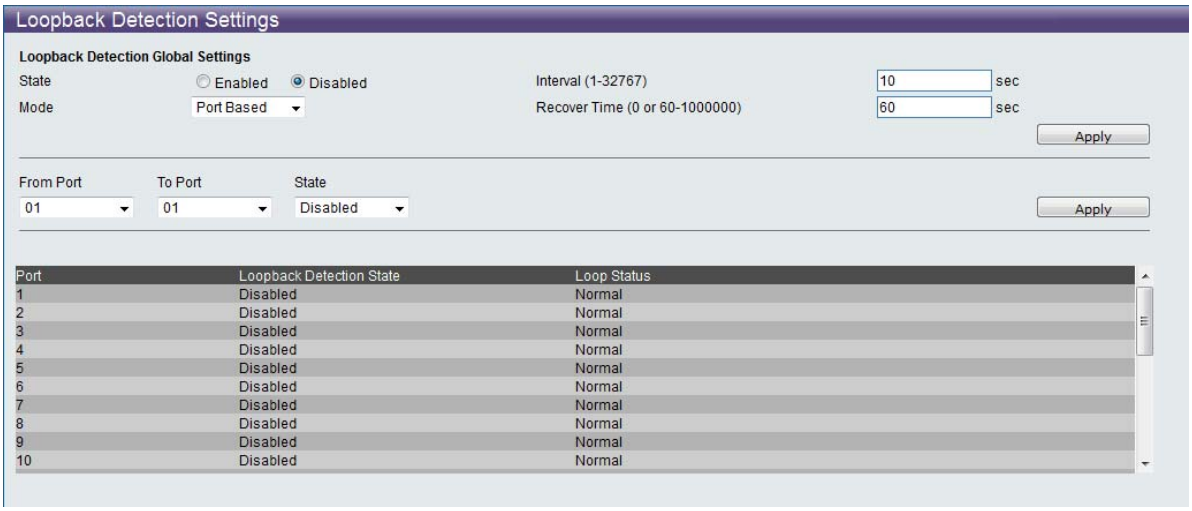
NOTE

You cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Also, the target port for the mirroring cannot be a member of a trunk group. Please note a target port and a source port cannot be the same port.

Loopback Detection Settings Page

On this page the user can configure the loopback dection settings.

To view this window, click **L2 Features > Loopback Detection Settings**:



In this window, the following parameters can be configured:

Parameter	Description
State	Here the user can enable or disable the loopback detection feature.
Interval	The time interval (in seconds) at which a device transmits all the CTP (Configuration Test Protocol) packets to detect the loopback event. The valid range is 1 to 32767. The default setting is 10.
Mode	The loopback detection port-based mode. In the port-based mode, the port will be disabled when a loop is detected.
Recover Time	The time interval (in seconds) used by the Auto-Recovery mechanism to decide how long to check if the loop status is gone. Zero is a special value which means to disable the auto-recovery mechanism; hence, a user needs to recover the disabled port back manually. The default value of the recover timer is 60. The valid range is 60 to 1000000.
From Port – To Port:	Specifies a range of ports to be configured for loopback detection status.

Click on the **Apply** button to accept the changes made.

Spanning Tree Folder

This Switch supports three versions of the Spanning Tree Protocol: STP, Rapid STP, and MSTP. STP will be familiar to most networking professionals. However, since RSTP and MSTP have been recently introduced to Extreme Networks managed Ethernet switches, a brief introduction to the technology is provided below, followed by a description of how to set up STP, RSTP, and MSTP.

802.1Q-2005 MSTP

Multiple Spanning Tree Protocol, or MSTP, is a standard defined by the IEEE community that allows multiple VLANs to be mapped to a single spanning tree instance, which will provide multiple pathways across the network. Therefore, these MSTP configurations will balance the traffic load, preventing wide scale disruptions when a single spanning tree instance fails. This will allow for faster convergences of new topologies for the failed instance. Frames designated for these VLANs will be

processed quickly and completely throughout interconnected bridges utilizing any of the three spanning tree protocols (STP, RSTP or MSTP).

This protocol will also tag BPDU packets so receiving devices can distinguish spanning tree instances, spanning tree regions and the VLANs associated with them. An MSTI ID will classify these instances. MSTP will connect multiple spanning trees with a Common and Internal Spanning Tree (CIST). The CIST will automatically determine each MSTP region, its maximum possible extent and will appear as one virtual bridge that runs a single spanning tree. Consequentially, frames assigned to different VLANs will follow different data routes within administratively established regions on the network, continuing to allow simple and full processing of frames, regardless of administrative errors in defining VLANs and their respective spanning trees.

Each switch utilizing the MSTP on a network will have a single MSTP configuration that will have the following three attributes:

1 A configuration name defined by an alphanumeric string of up to 32 characters (defined in the **MST Configuration Identification** window in the Configuration Name field).

2 A configuration revision number (named here as a Revision Level and found in the **MST Configuration Identification** window) and;

3 A 4094-element table (defined here as a VID List in the **MST Configuration Identification** window), which will associate each of the possible 4094 VLANs supported by the Switch for a given instance.

To utilize the MSTP function on the Switch, three steps need to be taken:

1 The Switch must be set to the MSTP setting (found in the **STP Bridge Global Settings** window in the STP Version field)

2 The correct spanning tree priority for the MSTP instance must be entered (defined here as a Priority in the **STP Instance Settings** window when configuring MSTI ID settings).

3 VLANs that will be shared must be added to the MSTP Instance ID (defined here as a VID List in the **MST Configuration Identification** window when configuring an MSTI ID settings).

Rapid Spanning Tree

The Switch implements three versions of the Spanning Tree Protocol, the Multiple Spanning Tree Protocol (MSTP) as defined by the IEEE 802.1Q-2005, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1D-2004 specification and a version compatible with the IEEE 802.1D-1998 STP. RSTP can operate with legacy equipment implementing IEEE 802.1D-1998; however the advantages of using RSTP will be lost.

The Rapid Spanning Tree Protocol (RSTP) evolved from the STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 functions that are increasingly handled by Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

Port Transition States

An essential difference between the three protocols is in the way ports transition to a forwarding state and in the way this transition relates to the role of the port (forwarding or not forwarding) in the topology. MSTP and RSTP combine the transition states disabled, blocking and listening used in STP and creates a single state Discarding. In either case, ports do not forward packets. In the STP port transition states disabled, blocking or listening or in the RSTP/MSTP port state discarding, there is no functional difference, the port is not active in the network topology. The table below compares how the three protocols differ regarding the port state transition.

All three protocols calculate a stable topology in the same way. Every segment will have a single path to the root bridge. All bridges listen for BPDU packets. However, BPDU packets are sent more frequently - with every Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and thus faster topology adjustment. A drawback of STP is this absence of immediate feedback from adjacent bridges.

MSTP	RSTP	STP	Forwarding	Learning
Disabled	Disabled	Disabled	No	No
Discarding	Discarding	Blocking	No	No
Discarding	Discarding	Listening	No	No
Learning	Learning	Learning	No	**Yes**
Forwarding	**Forwarding**	**Forwarding**	**Yes**	**Yes**

RSTP is capable of a more rapid transition to a forwarding state - it no longer relies on timer configurations - RSTP compliant bridges are sensitive to feedback from other RSTP compliant bridge links. Ports do not need to wait for the topology to stabilize before transitioning to a forwarding state. In order to allow this rapid transition, the protocol introduces two new variables: the edge port and the point-to-point (P2P) port.

Edge Port

The edge port is a configurable designation used for a port that is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

P2P Port

A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP/MSTP, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden through configuration.

STP/RSTP/MSTP Compatibility

MSTP or RSTP can interoperate with legacy equipment and is capable of automatically adjusting BPDU packets to STP format when necessary. However, any segment using STP will not benefit from the rapid transition and rapid topology change detection of MSTP or RSTP. The protocol also provides for a variable used for migration in the event that legacy equipment on a segment is updated to use RSTP or MSTP.

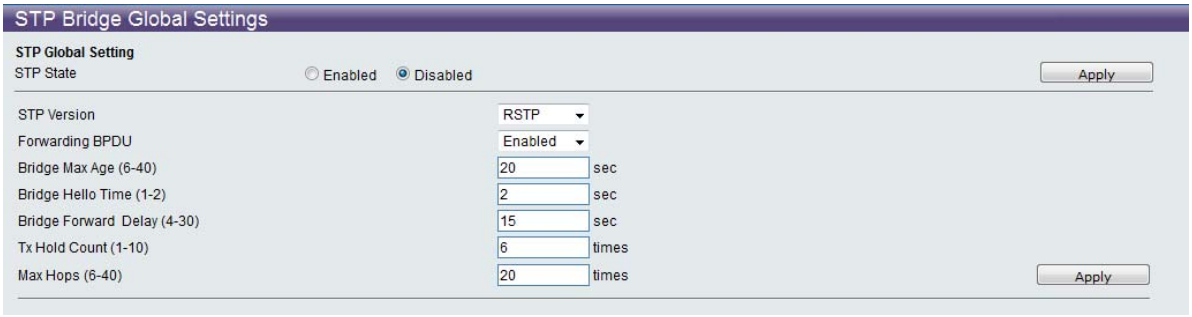
The Spanning Tree Protocol (STP) operates on two levels:

1 On the switch level, the settings are globally implemented.

2 On the port level, the settings are implemented on a per user-defined group of ports basis.

STP Bridge Global Settings

To open the following window, click **L2 features > Spanning Tree > STP Bridge Global Settings:**



In this window, the following parameters can be configured:

Parameter	Description
STP State	Use the radio buttons to enable or disable the STP Status.
STP Version	Use the pull-down menu to choose the desired version of STP to be implemented on the Switch. There are three choices: *STP* - Select this parameter to set the Spanning Tree Protocol (STP) globally on the switch. *RSTP* - Select this parameter to set the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. *MSTP* - Select this parameter to set the Multiple Spanning Tree Protocol (MSTP) globally on the Switch.
Forwarding BPDU	This field can be *Enabled* or *Disabled*. When *Enabled,* it allows the forwarding of STP BPDU packets from other network devices. The default is *Enabled*.
Bridge Max Age (6-40)	The Max Age may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your switch has the lowest Bridge Identifier, it will become the Root Bridge. The user may choose a time between *6* and *40* seconds. The default value is *20*.
Bridge Hello Time (1 – 2 Sec)	The Hello Time can be set from 1 to 2 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. **Note:** The Global Bridge Hello Time is only configurable if the DUT function is running in STP/RSTP mode.
Bridge Forward Delay (4-30)	The Forward Delay can be from *4* to *30* seconds. Any port on the Switch spends this time in the listening state while moving from the blocking state to the forwarding state.
Tx Hold Count (1-10)	Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from *1* to *10*. The default is *6*.
Max Hops (6-40)	Used to set the number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BPDU packet and the information held for the port will age out. The user may set a hop count from *6* to *40*. The default is *20*.

Click on the **Apply** button to accept the changes made.

NOTE

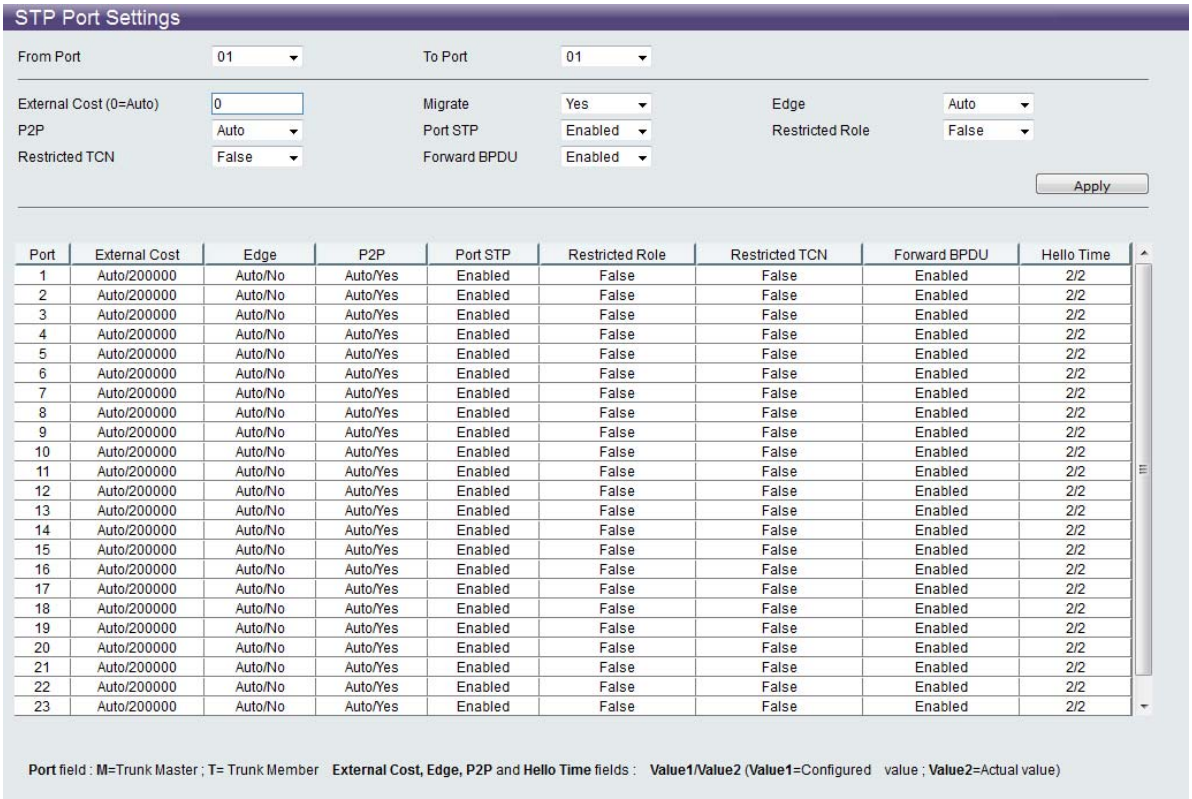
The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur. Observe the following formulas when setting the above parameters:

Max. Age ? 2 x (Forward Delay - 1 second)
Max. Age ? 2 x (Hello Time + 1 second)

STP Port Settings

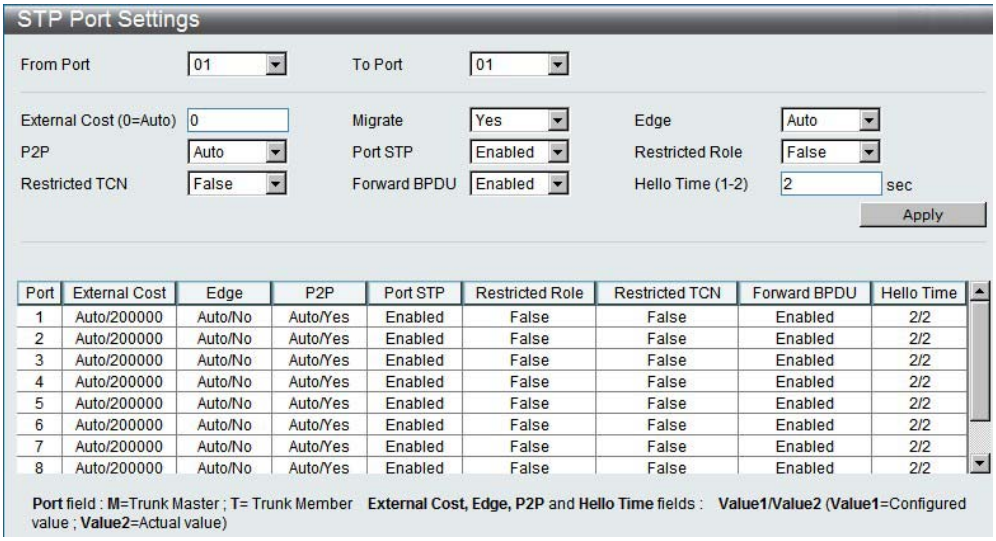
STP can be set up on a port per port basis.

To view the following window, click **L2 Features > Spanning Tree > STP Port Settings:**


STP Port Settings
From Port 01
To Port 01
External Cost (0=Auto) 0
Migrate Yes
Edge Auto
P2P Auto
Port STP Enabled
Restricted Role False
Restricted TCN False
Forward BPDU Enabled
Apply
Port | External Cost | Edge | P2P | Port STP | Restricted Role | Restricted TCN | Forward BPDU | Hello Time
1 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
2 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
3 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
4 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
5 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
6 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
7 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
8 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
9 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
10 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
11 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
12 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
13 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
14 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
15 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
16 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
17 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
18 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
19 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
20 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
21 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
22 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
23 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
Port field : M=Trunk Master ; T= Trunk Member External Cost, Edge, P2P and Hello Time fields : Value1/Value2 (Value1=Configured value ; Value2=Actual value)

NOTE

STP Port Settings window for RSTP/STP mode.


STP Port Settings
From Port
01
To Port
01
External Cost (0=Auto)
0
Migrate
Yes
Edge
Auto
P2P
Auto
Port STP
Enabled
Restricted Role
False
Restricted TCN
False
Forward BPDU
Enabled
Hello Time (1-2)
2
sec
Apply
Port | External Cost | Edge | P2P | Port STP | Restricted Role | Restricted TCN | Forward BPDU | Hello Time
1 | Auto/200000 | Auto/No | Auto/Yes | Enabled | False | False | Enabled | 2/2
2 | Auto/200000 | Auto/No | Auto/Yes | Enabled | False | False | Enabled | 2/2
3 | Auto/200000 | Auto/No | Auto/Yes | Enabled | False | False | Enabled | 2/2
4 | Auto/200000 | Auto/No | Auto/Yes | Enabled | False | False | Enabled | 2/2
5 | Auto/200000 | Auto/No | Auto/Yes | Enabled | False | False | Enabled | 2/2
6 | Auto/200000 | Auto/No | Auto/Yes | Enabled | False | False | Enabled | 2/2
7 | Auto/200000 | Auto/No | Auto/Yes | Enabled | False | False | Enabled | 2/2
8 | Auto/200000 | Auto/No | Auto/Yes | Enabled | False | False | Enabled | 2/2
Port field : M=Trunk Master ; T= Trunk Member
External Cost, Edge, P2P and Hello Time fields : Value1/Value2 (Value1=Configured value ; Value2=Actual value)

NOTE

STP Port Settings window for MSTP mode.

In addition to setting Spanning Tree parameters for use on the switch level, the Switch allows for the configuration of groups of ports, each port-group of which will have its own spanning tree, and will require some of its own configuration settings. An STP Group will use the switch-level parameters entered above, with the addition of Port Priority and Port Cost.

An STP Group spanning tree works in the same way as the switch-level spanning tree, but the root bridge concept is replaced with a root port concept. A root port is a port of the group that is elected based on port priority and port cost, to be the connection to the network for the group. Redundant links will be blocked, just as redundant links are blocked on the switch level.

The STP on the switch level blocks redundant links between switches (and similar network devices). The port level STP will block redundant links within an STP Group.

It is advisable to define an STP Group to correspond to a VLAN group of ports.

In this window, the following parameters can be configured:

Parameter	Description
From Port/To Port	A consecutive group of ports may be configured starting with the selected port.
External Cost (0=Auto)	External Cost - This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is *0* (auto). *0 (auto)* - Setting *0* for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = *200000*. Gigabit port = *20000*. *value 1-200000000* - Define a value between *1* and *200000000* to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.

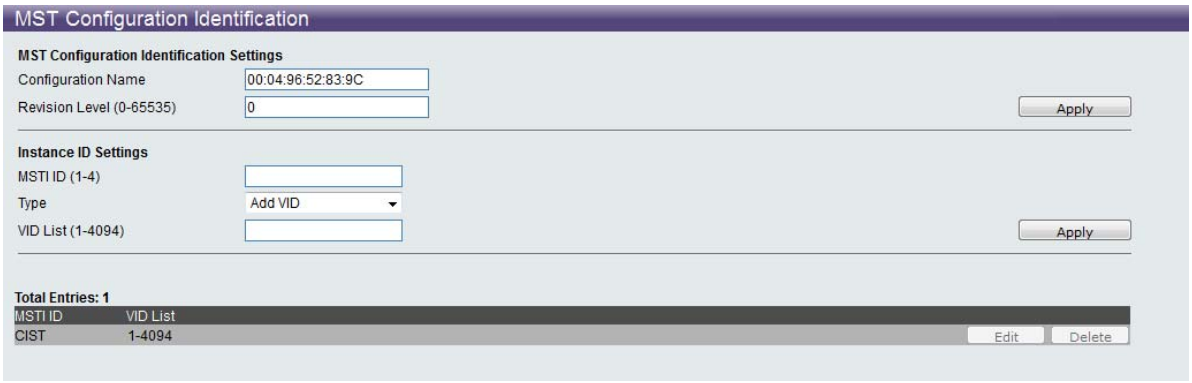
Parameter	Description
Migrate	Setting this parameter as *Yes* will set the ports to send out BPDU packets to other bridges, requesting information on their STP setting If the Switch is configured for RSTP, the port will be capable to migrate from 802.1D STP to 802.1w RSTP. Migration should be set as yes on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP on all or some portion of the segment.
Edge	Choosing the *True* parameter designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received, it automatically loses edge port status. Setting the value to *true* under STP mode has no effect. Choosing the *Auto* parameter will indicate that the port will be able to automatically enable edge port status if needed.
P2P	Choosing the *True* parameter indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports, however they are restricted in that a P2P port must operate in full-duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A P2P value of *false* indicates that the port cannot have P2P status. *Auto* allows the port to have P2P status whenever possible and operate as if the P2P status were true. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the P2P status changes to operate as if the P2P value were *False*. The default setting for this parameter is *Auto*.
Port STP	Allows STP to be *Enabled* or *Disabled* for the ports.
Restricted Role	Toggle between *True* and *False* to set the restricted role state of the packet. The default value is *False*.
Restricted TCN	Toggle between *True* and *False* to set the restricted TCN of the packet. The default value is *False*.
Forward BPDU	This field can be *Enabled* or *Disabled.* When *Enabled,* it allows the forwarding of STP BPDU packets from other network devices. The default is *Enabled*.
Hello Time (1–2)	The Hello Time can be set from *1* to *2* seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. The default value is *2*. **Note:** Hello Time is only configurable per port if DUT is running in MSTP mode.

Click on the **Apply** button to accept the changes made.

MST Configuration Identification

The following windows in the MST Configuration Identification section allow the user to configure a MSTI instance on the Switch. These settings will uniquely identify a multiple spanning tree instance set on the Switch. The Switch initially possesses one *CIST* or Common Internal Spanning Tree of which the user may modify the parameters for but cannot change the MSTI ID for, and cannot be deleted.

To view this window, click **L2 Features > Spanning Tree > MST Configuration Identification:**



In this window, the following parameters can be configured:

Parameter	Description
Configuration Name	A previously configured name set on the Switch to uniquely identify the MSTI (Multiple Spanning Tree Instance). If a configuration name is not set, this field will show the MAC address to the device running MSTP. This field can be set in the **STP Bridge Global Settings** window.
Revision Level (0-65535)	This value, along with the Configuration Name will identify the MSTP region configured on the Switch. The user may choose a value between *0* and *65535* with a default setting of *0*.
MSTI ID (1-4)	This field shows the MSTI IDs currently set on the Switch. This field will always have the CIST MSTI, which may be configured but not deleted.
Type	This field allows the user to choose a desired method for altering the MSTI settings. The user has two choices. *Add VID* - Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter. *Remove VID* - Select this parameter to remove VIDs from the MSTI ID, in conjunction with the VID List parameter.
VID List (1-4094)	This field displays the VLAN IDs associated with the specific MSTI.

Click on the **Apply** button to accept the changes made.

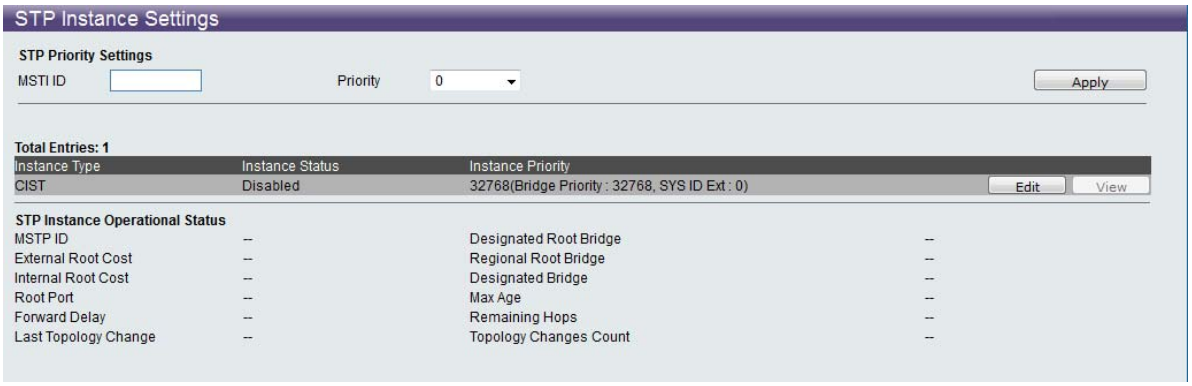
Click on the **Edit** button to re-configure a specific entry.

Click on the **Delete** button to remove the selected entry.

STP Instance Settings

The following window displays MSTIs currently set on the Switch.

To view the following table, click **L2 Features > Spanning Tree > STP Instance Settings:**



In this window, the following parameters can be configured:

Parameter	Description
MSTI ID	Displays the MSTI ID of the instance being modified. An entry of *0* in this field denotes the CIST (default MSTI).
Priority	Enter the new priority in the Priority field. The user may set a priority value between *0* and *61440*.

Click on the **Apply** button to accept the changes made.

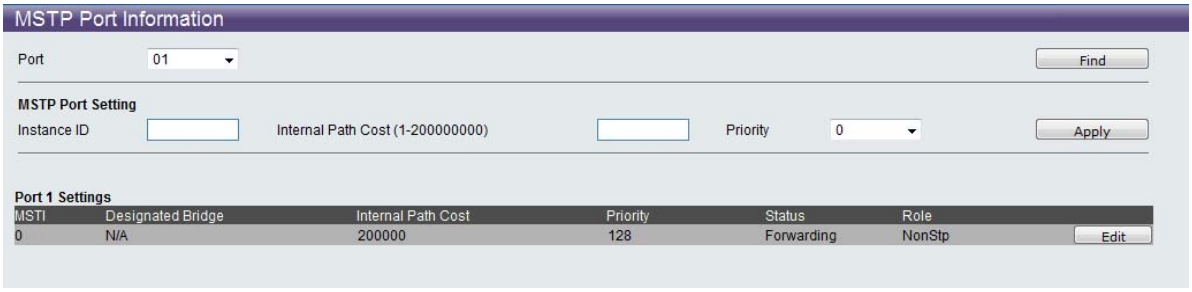
Click on the **Edit** button to re-configure a specific entry.

To see the STP Instance Operational Status of a previously configured setting, click **View**.

MSTP Port Information

This window displays the current MSTP Port Information and can be used to update the port configuration for an MSTI ID. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked. Remember that lower priority values mean higher priorities for forwarding packets.

To view the following window, click **L2 Features > Spanning Tree > MSTP Port Information:**



In this window, the following parameters can be configured:

Parameter	Description
Port	Use the drop-down menu to select a port.
Instance ID	Displays the MSTI ID of the instance being configured. An entry of *0* in this field denotes the CIST (default MSTI).
Internal Path Cost (1-200000000)	This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. A lower Internal cost represents a quicker transmission.
Priority	Select a value between *0* and *240* to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority.

Click on the **Find** button to find a specific entry based on the parameters entered.

Click on the **Apply** button to accept the changes made.

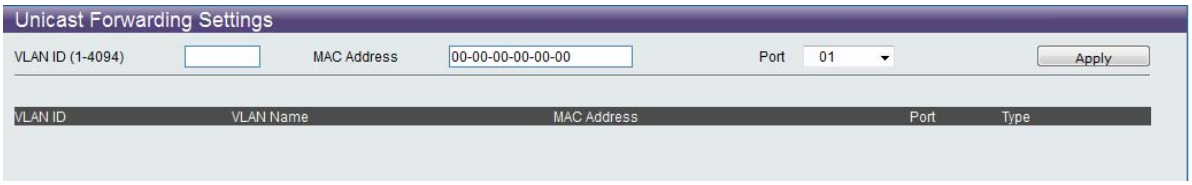
Click on the **Edit** button to re-configure a specific entry.

Forwarding & Filtering Folder

This folder contains windows for Unicast Forwarding and Multicast Forwarding.

Unicast Forwarding Settings

To view this window, click **L2 Features > Forwarding & Filtering > Unicast Forwarding Settings:**



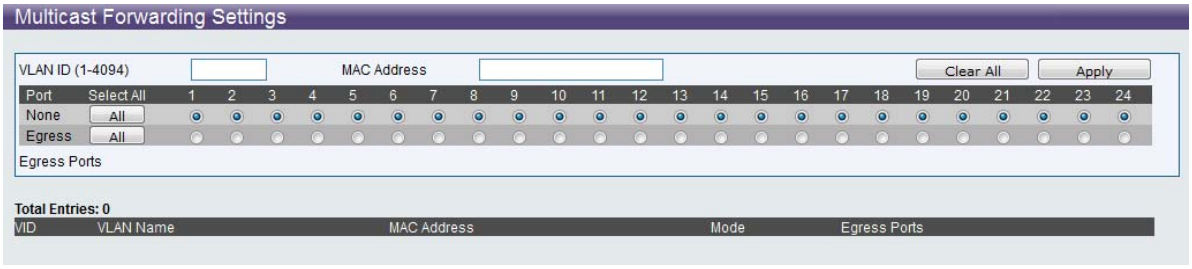
In this window, the following parameters can be configured:

Parameter	Description
VLAN ID (1-4094)	The VLAN ID number of the VLAN on which the above Unicast MAC address resides.
MAC Address	The MAC address to which packets will be statically forwarded. This must be a unicast MAC address.
Port	Select the port number on which the MAC address entered above resides.
VLAN Name	The VLAN Name associated with the subnet.

Click on the **Apply** button to accept the changes made.

Multicast Forwarding Settings

To view this window, click **L2 Features > Forwarding & Filtering > Multicast Forwarding Settings:**



In this window, the following parameters can be configured:

Parameter	Description
VLAN ID (1-4094)	The VLAN ID of the VLAN to which the corresponding MAC address belongs.
MAC Address	The MAC address that will be added to the multicast forwarding table.
Port Settings	Allows the selection of ports that will be members of the static multicast group. The options are: *None* - No restrictions on the port dynamically joining the multicast group. When None is chosen, the port will not be a member of the static multicast group. *Egress* - The port is a static member of the multicast group. Click **All** to choose either all of the ports selected as None or all of the ports selected as Egress. Click **Clear All** to clear all the settings at the top of this window.

Click on the **Apply** button to accept the changes made.

Click on the **Edit** button to re-configure a specific entry.

Click on the **Delete** button to remove the selected entry.

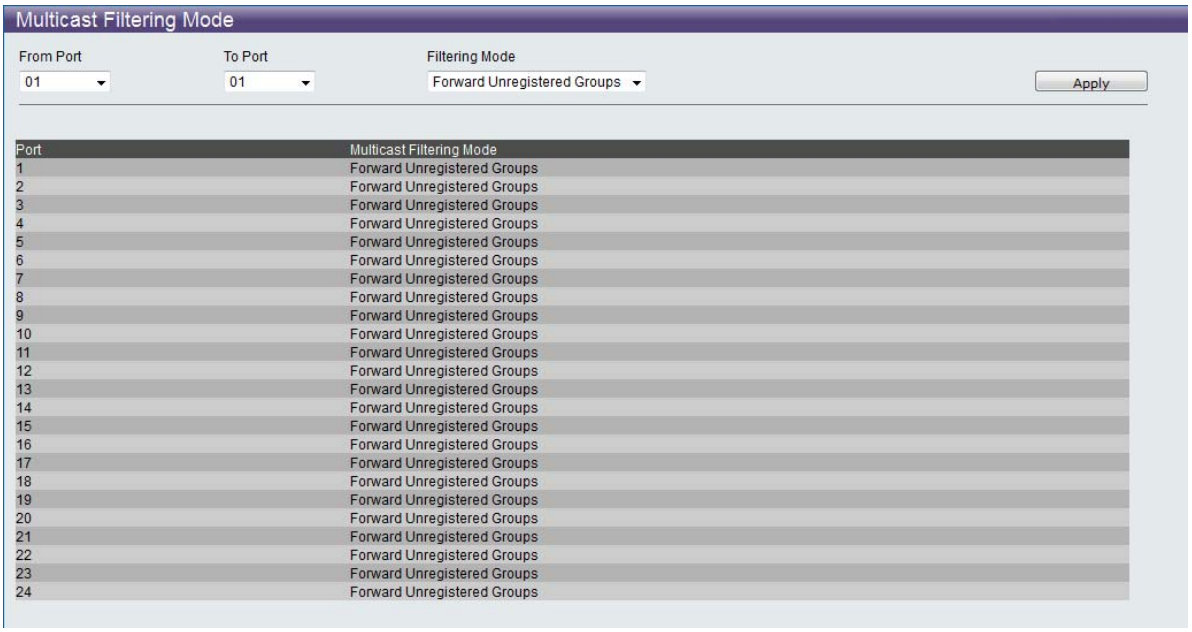
Click on the **Clear All** button to clear all the entered data from the fields.

Click on the **All** button to select all the ports for this configuration.

Multicast Filtering Mode

Users can configure the multicast filtering mode.

To view this window, click **L2 Features > Forwarding & Filtering > Multicast Filtering Mode:**



In this window, the following parameters can be configured:

Parameter	Description
From Port/To Port	The range of ports to be configured.
Filtering Mode	This drop-down menu instructs the Switch what action to take when it receives a multicast packet that requires forwarding to a port. *Forward Unregistered Groups* – This will instruct the Switch to forward a multicast packet whose destination is an unregistered multicast group residing within the range of ports specified above. *Filter Unregistered Groups* – This will instruct the Switch to filter any multicast packets whose destination is an unregistered multicast group residing within the range of ports specified above..

Click on the **Apply** button to accept the changes made.

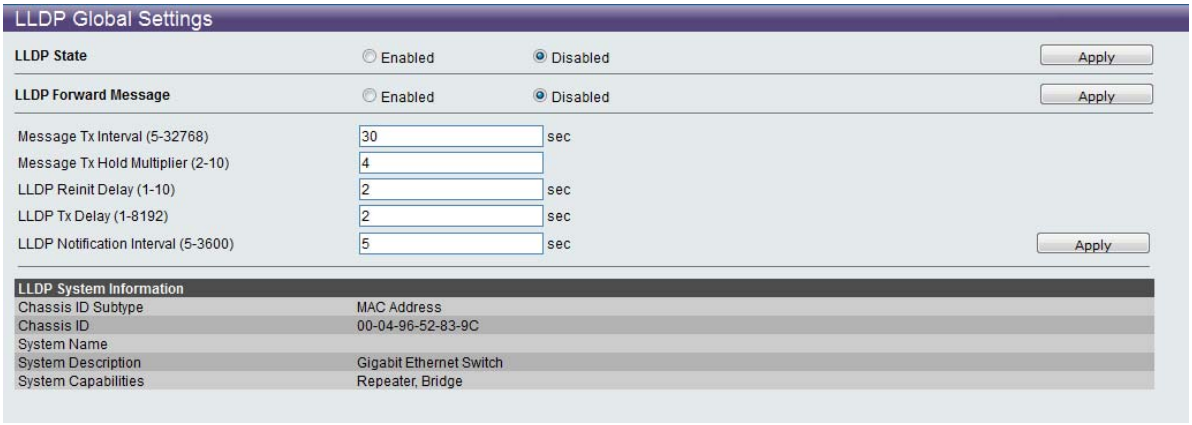
LLDP Folder

The Link Layer Discovery Protocol (LLDP) allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN. The major capabilities provided by this system is that it incorporates the station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station's point of attachment to the IEEE 802 LAN required by those management entity or entities.

The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) through a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP Global Settings

To view this window, click **L2 Features > LLDP > LLDP Global Settings:**



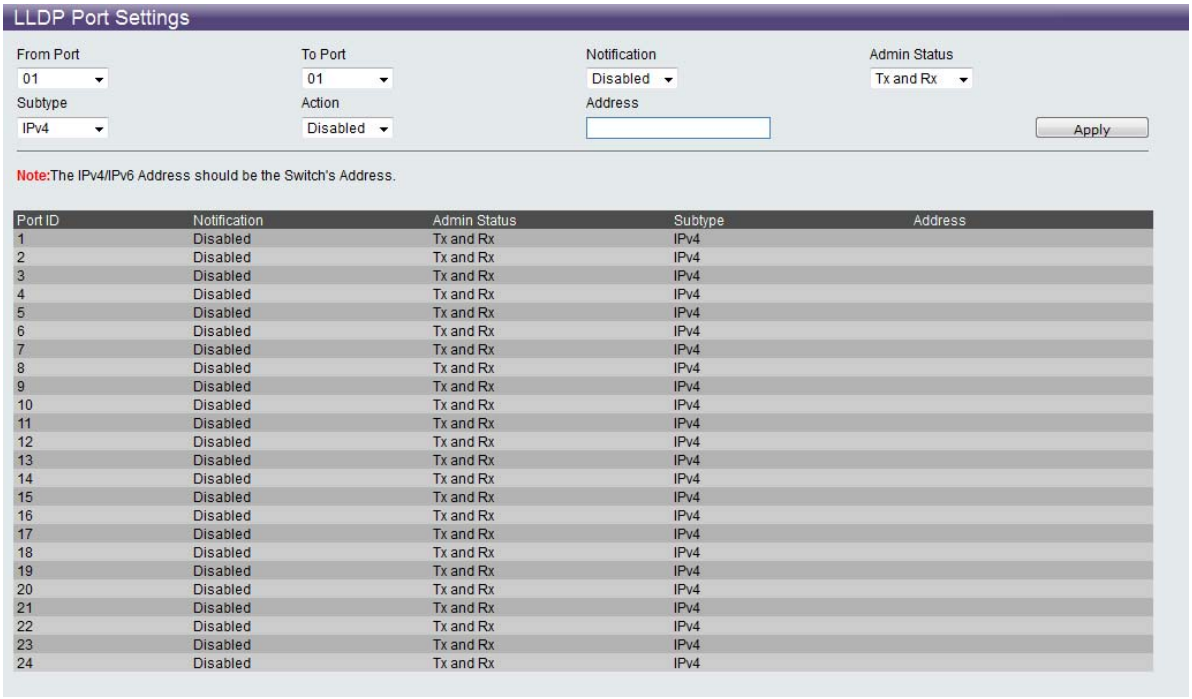
In this window, the following parameters can be configured:

Parameter	Description
LLDP State	Used to enable or disable LLDP on the Switch.
LLDP Forward Message	When LLDP is Disabled this function controls the LLDP packet forwarding message based on individual ports. If LLDP is enabled on a port it will flood the LLDP packet to all ports that have the same port VLAN and will advertise to other stations attached to the same IEEE 802 LAN.
Message Tx Interval (5-32768)	This interval controls how often active ports retransmit advertisements to their neighbors. To change the packet transmission interval, enter a value in seconds (*5* to *32768*).
Message Tx Hold Multiplier (2-10)	This function calculates the Time-to-Live for creating and transmitting the LLDP advertisements to LLDP neighbors by changing the multiplier used by an LLDP Switch. When the Time-to-Live for an advertisement expires the advertised data is then deleted from the neighbor Switch's MIB.
LLDP Reinit Delay (1-10)	The LLDP reinitialization delay interval is the minimum time that an LLDP port will wait before reinitializing after receiving an LLDP disable command. To change the LLDP Reinit Delay, enter a value in seconds (*1* to *10*).
LLDP Tx Delay (1-8192)	LLDP TX Delay allows the user to change the minimum time delay interval for any LLDP port which will delay advertising any successive LLDP advertisements due to change in the LLDP MIB content. To change the LLDP TX Delay, enter a value in seconds (*1* to *8192*).
LLDP Notification Interval (5-3600)	LLDP Notification Interval is used to send notifications to configured SNMP trap receiver(s) when an LLDP change is detected in an advertisement received on the port from an LLDP neighbor. To set the LLDP Notification Interval, enter a value in seconds (*5* to *3600*).

Click on the **Apply** button to accept the changes made.

LLDP Port Settings

To view this window, click **L2 Features > LLDP > LLDP Port Settings:**


LLDP Port Settings
From Port
01
To Port
01
Notification
Disabled
Admin Status
Tx and Rx
Subtype
IPv4
Action
Disabled
Address
Apply
Note:The IPv4/IPv6 Address should be the Switch's Address.
Port ID Notification Admin Status Subtype Address
1 Disabled Tx and Rx IPv4
2 Disabled Tx and Rx IPv4
3 Disabled Tx and Rx IPv4
4 Disabled Tx and Rx IPv4
5 Disabled Tx and Rx IPv4
6 Disabled Tx and Rx IPv4
7 Disabled Tx and Rx IPv4
8 Disabled Tx and Rx IPv4
9 Disabled Tx and Rx IPv4
10 Disabled Tx and Rx IPv4
11 Disabled Tx and Rx IPv4
12 Disabled Tx and Rx IPv4
13 Disabled Tx and Rx IPv4
14 Disabled Tx and Rx IPv4
15 Disabled Tx and Rx IPv4
16 Disabled Tx and Rx IPv4
17 Disabled Tx and Rx IPv4
18 Disabled Tx and Rx IPv4
19 Disabled Tx and Rx IPv4
20 Disabled Tx and Rx IPv4
21 Disabled Tx and Rx IPv4
22 Disabled Tx and Rx IPv4
23 Disabled Tx and Rx IPv4
24 Disabled Tx and Rx IPv4

In this window, the following parameters can be configured:

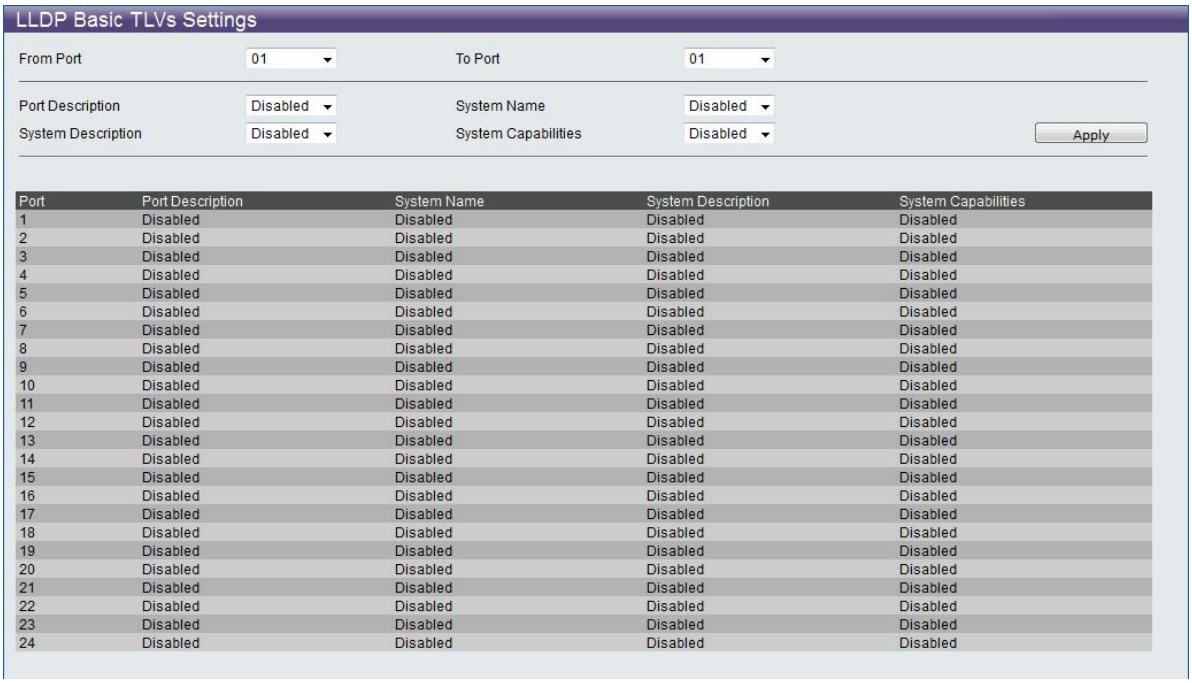
Parameter	Description
From Port/To Port	Use the pull-down menu to select a range of ports to be configured.
Notification	Use the pull-down menu to Enable or Disable the status of the LLDP notification. This function controls the SNMP trap, however it cannot implement traps on SNMP when the notification is disabled.
Admin Status	This functions controls the local LLDP agent and allows it to send and receive LLDP frames on the ports.This option contains *Tx*, *Rx*, *Tx and Rx* or *Disabled*. *Tx*: the local LLDP agent can only transmit LLDP frames. *Rx*: the local LLDP agent can only receive LLDP frames. *Tx and Rx*: the local LLDP agent can both transmit and receive LLDP frames. *Disabled*: the local LLDP agent can neither transmit nor receive LLDP frames. The defaut value is *Tx and Rx*.
Subtype	This read-only field displays IPv4, the type of the IP address.
Action	Used to *Enable* or *Disable* the advertise management address function base port.
Address	The address must be the management IP-address. For multi IP-addresses, you can enter any IP or create a new IP interface that you want to add.

Click on the **Apply** button to accept the changes made.

LLDP Basic TLVs Settings

This window is used to enable the settings for the Basic TLVs Settings.

To view this window, click **L2 Features > LLDP > LLDP Basic TLVs Settings:**



In this window, the following parameters can be configured:

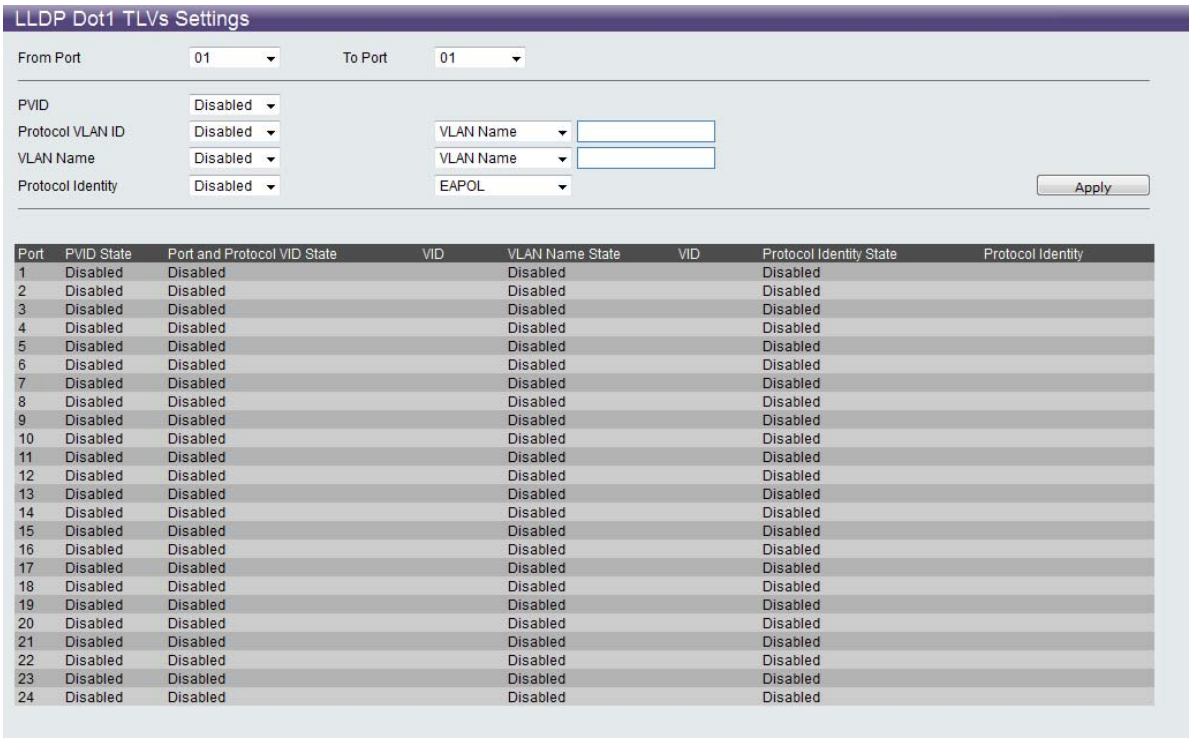
Parameter	Description
From Port/To Port	Use the pull-down menu to select a range of ports to be configured.
Port Description	Use the drop-down menu to enable or disable port description.
System Name	Use the drop-down menu to enable or disable system name.
System Description	Use the drop-down menu to enable or disable system description.
System Capabilities	Use the drop-down menu to enable or disable system capabilities.

Click on the **Apply** button to accept the changes made.

LLDP Dot1 TLVs Settings

LLDP Dot1 TLVs are organizationally specific TLVs which are defined in IEEE 802.1 and used to configure an individual port or group of ports to exclude one or more of the IEEE 802.1 organizational port VLAN ID TLV data types from outbound LLDP advertisements.

To view this window, click **L2 Features > LLDP > LLDP Dot1 TLVs Settings:**


LLDP Dot1 TLVs Settings
From Port
01
To Port
01
PVID
Disabled
Protocol VLAN ID
Disabled
VLAN Name
VLAN Name
Disabled
VLAN Name
Protocol Identity
Disabled
EAPOL
Apply
Port PVID State Port and Protocol VID State VID VLAN Name State VID Protocol Identity State Protocol Identity
1 Disabled Disabled Disabled Disabled
2 Disabled Disabled Disabled Disabled
3 Disabled Disabled Disabled Disabled
4 Disabled Disabled Disabled Disabled
5 Disabled Disabled Disabled Disabled
6 Disabled Disabled Disabled Disabled
7 Disabled Disabled Disabled Disabled
8 Disabled Disabled Disabled Disabled
9 Disabled Disabled Disabled Disabled
10 Disabled Disabled Disabled Disabled
11 Disabled Disabled Disabled Disabled
12 Disabled Disabled Disabled Disabled
13 Disabled Disabled Disabled Disabled
14 Disabled Disabled Disabled Disabled
15 Disabled Disabled Disabled Disabled
16 Disabled Disabled Disabled Disabled
17 Disabled Disabled Disabled Disabled
18 Disabled Disabled Disabled Disabled
19 Disabled Disabled Disabled Disabled
20 Disabled Disabled Disabled Disabled
21 Disabled Disabled Disabled Disabled
22 Disabled Disabled Disabled Disabled
23 Disabled Disabled Disabled Disabled
24 Disabled Disabled Disabled Disabled

In this window, the following parameters can be configured:

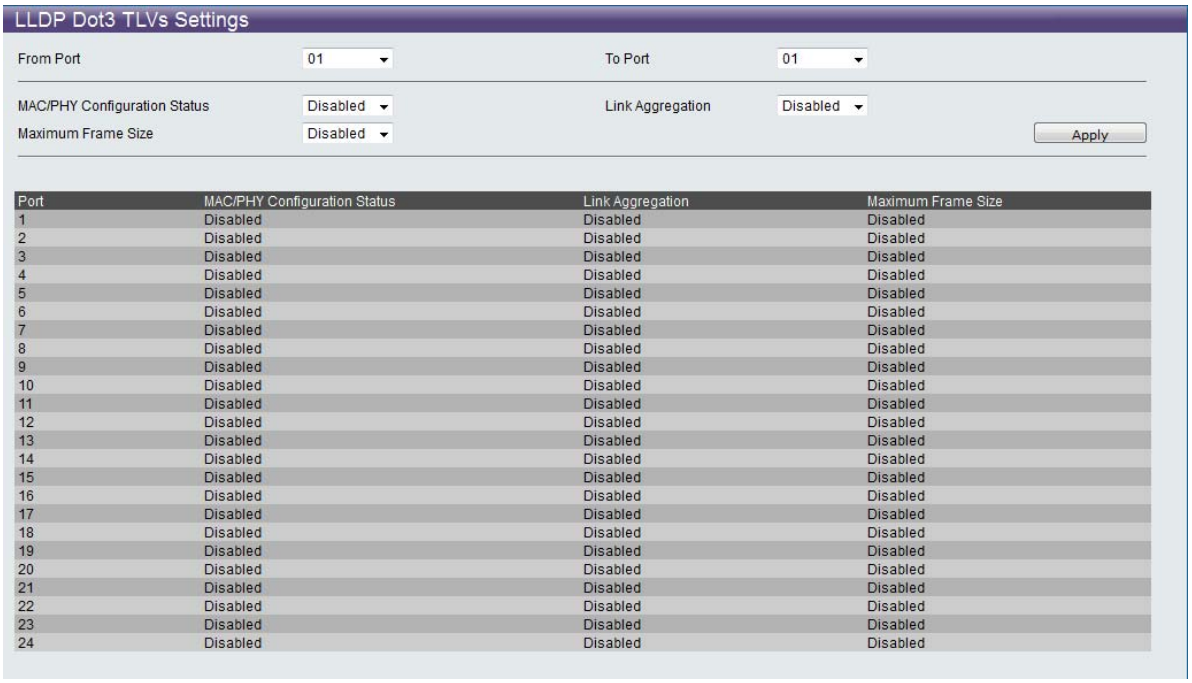
Parameter	Description
From Port/To Port	Use the pull-down menu to select a range of ports to be configured.
PVID	Use the drop-down menu to enable or disable the advertise PVID.
Protocol VLAN ID	Use the drop-down menu to enable or disable the advertise Protocol VLAN ID.
VLAN Name	Use the drop-down menu to enable or disable the advertise VLAN Name.
Protocol Identity	Use the drop-down menu to enable or disable the advertise Protocol Identity.

Click on the **Apply** button to accept the changes made.

LLDP Dot3 TLVs Settings

This window is used to configure an individual port or group of ports to exclude one or more IEEE 802.3 organizational specific TLV data type from outbound LLDP advertisements.

To view this window, click **L2 Features > LLDP > LLDP Dot3 TLVs Settings:**



In this window, the following parameters can be configured:

Parameter	Description
From Port / To Port	Use the drop-down menu to select a range of ports to be configured.
MAC/PHY Configuration Status	This TLV optional data type indicates that the LLDP agent should transmit 'MAC/PHY configuration/status TLV'. This indicates it is possible for two ends of an IEEE 802.3 link to be configured with different duplex and/or speed settings and still establish some limited network connectivity. More precisely, the information includes whether the port supports the auto-negotiation function, whether the function is enabled, whether it has auto-negotiated advertised capability, and what is the operational MAU type. The default state is *Disabled*.
Link Aggregation	The Link Aggregation option indicates that LLDP agents should transmit 'Link Aggregation TLV'. This indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in an aggregated link, and what is the aggregated port ID. The default state is *Disabled*.
Maximum Frame Size	The Maximum Frame Size indicates that LLDP agent should transmit 'Maximum-frame-size TLV. The default state is *Disabled*.

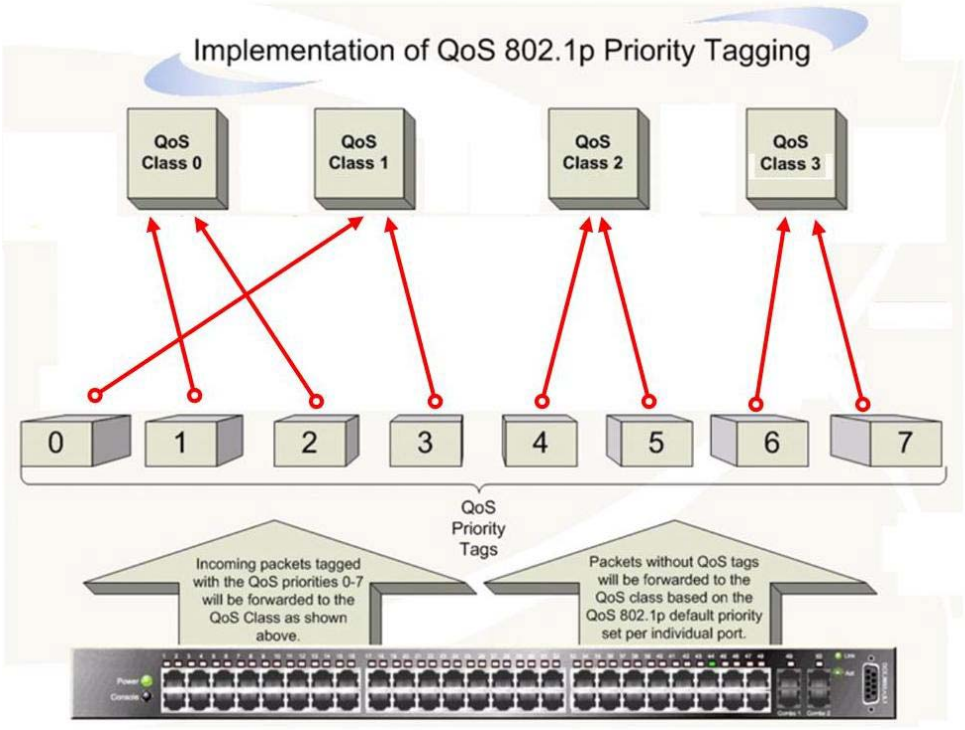
Click on the **Apply** button to accept the changes made.

4 CHAPTER Quality of Service (QoS)

The Switch supports 802.1p priority queuing Quality of Service. The following section discusses the implementation of QoS (Quality of Service) and benefits of using 802.1p priority queuing.

Advantages of QoS

QoS is an implementation of the IEEE 802.1p standard that allows network administrators a method of reserving bandwidth for important functions that require a large amount of bandwidth or have a high priority, such as VoIP (Voice-over Internet Protocol), Web browsing applications, file server applications or video conferencing. Not only can larger bandwidth be created, but other less critical traffic can be limited, so excessive bandwidth can be saved. The Switch has separate hardware queues on every physical port to which packets from various applications can be mapped to, and, in turn prioritized. View the following map to see how the Switch implements 802.1P priority queuing.


Implementation of QoS 802.1p Priority Tagging
QoS Class 0
QoS Class 1
QoS Class 2
QoS Class 3
0
1
2
3
4
5
6
7
QoS Priority Tags
Incoming packets tagged with the QoS priorities 0-7 will be forwarded to the QoS Class as shown above.
Packets without QoS tags will be forwarded to the QoS class based on the QoS 802.1p default priority set per individual port.

The previous picture shows the default priority setting for the Switch. Class 3 has the highest priority of the four priority queues on the Switch. In order to implement QoS, the user is required to instruct the Switch to examine the header of a packet to see if it has the proper identifying tag tagged. Then the user may forward these tagged packets to designated queues on the Switch where they will be emptied, based on priority.

For example, if a user wishes to have a videoconference between two remotely set computers, the administrator can add priority tags to the video packets being sent out, utilizing the Access Profile commands. Then, on the receiving end, the administrator instructs the Switch to examine packets for this tag, acquires the tagged packets and maps them to a class queue on the Switch. Then in turn, the administrator will set a priority for this queue so that will be emptied before any other packet is forwarded. This result for the end user is receiving all packets sent as quickly as possible, thus prioritizing the queue and allowing for an uninterrupted stream of packets, which optimizes the use of bandwidth available for the video conference.

Understanding QoS

The Switch has four priority queues. These priority queues are labeled from 0 to 3, with 3 being the highest priority and 0 the lowest priority queue. The eight priority tags, specified in IEEE 802.1p are mapped to the Switch's priority tags as follows:

- Priority 0 is assigned to the Switch's Q1 queue.
- Priority 1 is assigned to the Switch's Q0 queue.
- Priority 2 is assigned to the Switch's Q0 queue.
- Priority 3 is assigned to the Switch's Q1 queue.
- Priority 4 is assigned to the Switch's Q2 queue.
- Priority 5 is assigned to the Switch's Q2 queue.
- Priority 6 is assigned to the Switch's Q3 queue.
- Priority 7 is assigned to the Switch's Q3 queue.

For strict priority-based scheduling, any packets residing in the higher priority queues are transmitted first. Multiple strict priority queues empty based on their priority tags. Only when these queues are empty, are packets of lower priority transmitted.

For weighted round robin queuing, the number of packets sent from each priority queue depends upon the assigned weight. For a configuration of four QoS queues, A~D with their respective weight value: 4~1, the packets are sent in the following sequence: A1, B1, C1, D1, A2, B2, C2, A3, B3, A4.

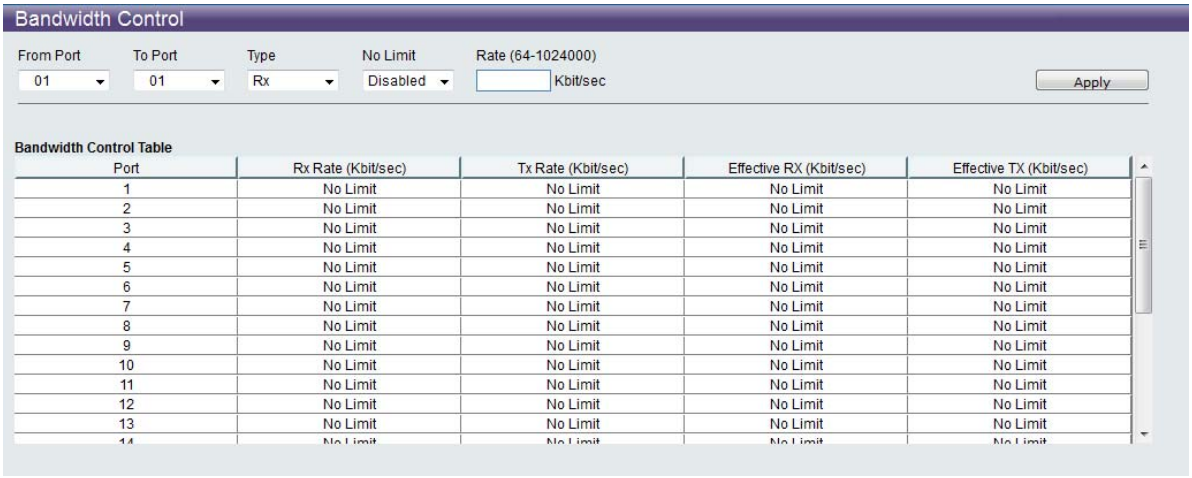
For weighted round robin queuing, if each QoS queue has the same weight value, then each QoS queue has an equal opportunity to send packets just like round robin queuing.

The Switch has four priority queues (and eight Classes of Service) for each port.

Bandwidth Control

The bandwidth control settings are used to place a ceiling on the transmitting and receiving data rates for any selected port.

To view this window, click **QoS > Bandwidth Control**:


Bandwidth Control
From Port
To Port
Type
No Limit
Rate (64-1024000)
01
01
Rx
Disabled
Kbit/sec
Apply
Bandwidth Control Table
Port
Rx Rate (Kbit/sec)
Tx Rate (Kbit/sec)
Effective RX (Kbit/sec)
Effective TX (Kbit/sec)
1 No Limit No Limit No Limit No Limit
2 No Limit No Limit No Limit No Limit
3 No Limit No Limit No Limit No Limit
4 No Limit No Limit No Limit No Limit
5 No Limit No Limit No Limit No Limit
6 No Limit No Limit No Limit No Limit
7 No Limit No Limit No Limit No Limit
8 No Limit No Limit No Limit No Limit
9 No Limit No Limit No Limit No Limit
10 No Limit No Limit No Limit No Limit
11 No Limit No Limit No Limit No Limit
12 No Limit No Limit No Limit No Limit
13 No Limit No Limit No Limit No Limit

In this window, the following parameters can be configured:

Parameter	Description
From Port/To Port	A consecutive group of ports may be configured starting with the selected port.
Type	This drop-down menu allows you to select between *Rx* (receive), *Tx (*transmit), and *Both*. This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.
No Limit	Use the drop-down menu to specify the selected port has limited or unlimited bandwidth.
Rate (64–1024000)	This field allows you to enter the data rate, in Kbits per second, that will be the limit for the selected port. The value must be a multiple of 64, between *64* and *1024000*.

Click on the **Apply** button to accept the changes made.

Traffic Control

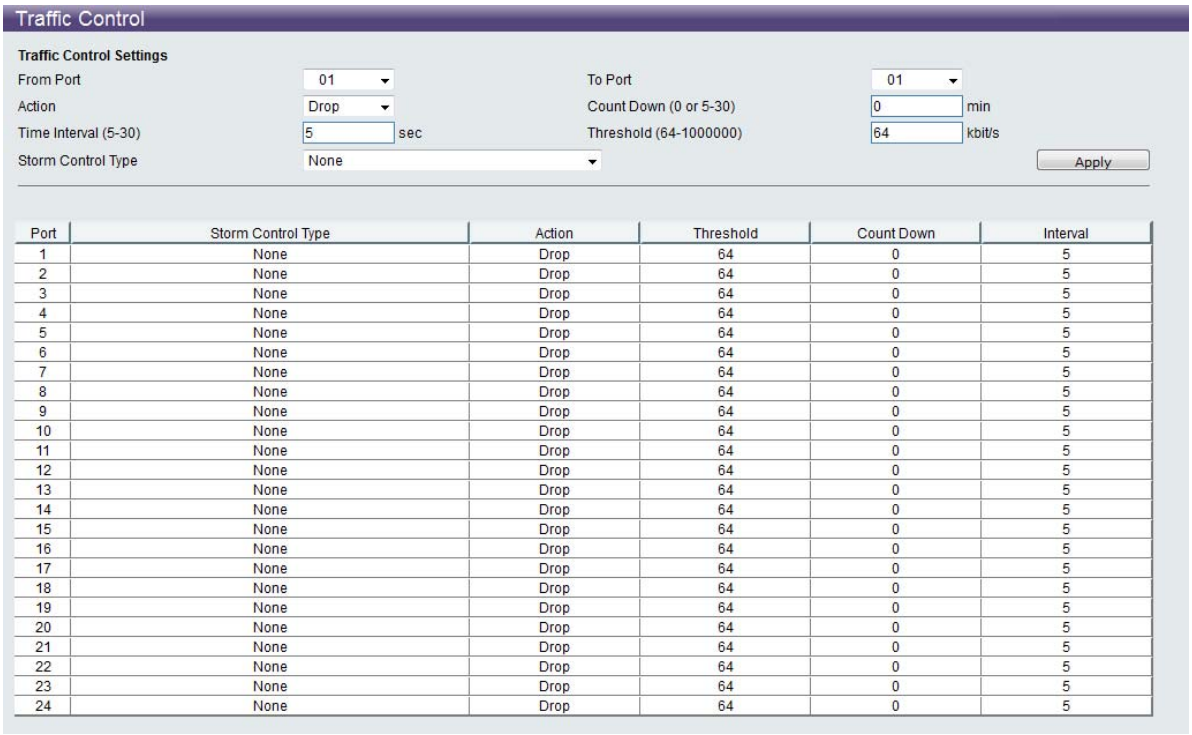
On a computer network, packets such as Multicast packets and Broadcast packets continually flood the network as normal procedure. At times, this traffic may increase due to a malicious endstation on the network or a malfunctioning device, such as a faulty network card. Thus, switch throughput problems will arise and consequently affect the overall performance of the switch network. To help rectify this packet storm, the Switch will monitor and control the situation.

The packet storm is monitored to determine if too many packets are flooding the network, based on the threshold level provided by the user. Once a packet storm has been detected, the Switch will drop

packets coming into the Switch until the storm has subsided. This method can be utilized by selecting the Drop option of the Action field in the window below.

The Switch will also scan and monitor packets coming into the Switch by monitoring the Switch's chip counter. This method is only viable for Broadcast and Multicast storms because the chip only has counters for these two types of packets. Once a storm has been detected (that is, once the packet threshold set below has been exceeded), the Switch will shutdown the port to all incoming traffic with the exception of STP BPDU packets, for a time period specified using the CountDown field. If the packet storm discontinues before the Countdown timer expires, the port will again allow all incoming traffic. If this field times out and the packet storm continues, the port will be placed in a Shutdown Rest mode which will produce a warning message recorded in the log. Once in Shutdown Rest mode, the port will be recovered after 5 minutes, or the user manually resets the port using the **Port Configuration** window in the **Configuration** folder and selecting the disabled port and returning it to an Enabled status. To utilize this method of Storm Control, choose the Shutdown option of the Action field in the window below.

To view this window, click **QoS > Traffic Control**:


Traffic Control
Traffic Control Settings
From Port 01
To Port 01
Action Drop
Count Down (0 or 5-30) 0 min
Time Interval (5-30) 5 sec
Threshold (64-1000000) 64 kbit/s
Storm Control Type None
Apply
Port Storm Control Type Action Threshold Count Down Interval
1 None Drop 64 0 5
2 None Drop 64 0 5
3 None Drop 64 0 5
4 None Drop 64 0 5
5 None Drop 64 0 5
6 None Drop 64 0 5
7 None Drop 64 0 5
8 None Drop 64 0 5
9 None Drop 64 0 5
10 None Drop 64 0 5
11 None Drop 64 0 5
12 None Drop 64 0 5
13 None Drop 64 0 5
14 None Drop 64 0 5
15 None Drop 64 0 5
16 None Drop 64 0 5
17 None Drop 64 0 5
18 None Drop 64 0 5
19 None Drop 64 0 5
20 None Drop 64 0 5
21 None Drop 64 0 5
22 None Drop 64 0 5
23 None Drop 64 0 5
24 None Drop 64 0 5

In this window, the following parameters can be configured:

Parameter	Description
From Port/To Port	A consecutive group of ports may be configured starting with the selected port.

Parameter	Description
Action	Select the method of traffic Control from the pull-down menu. The choices are: *Drop* – Utilizes the hardware Traffic Control mechanism, which means the Switch's hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved. *Shutdown* – Utilizes the Switch's software Traffic Control mechanism to determine the Packet Storm occurring. Once detected, the port will deny all incoming traffic to the port except STP BPDU packets, which are essential in keeping the Spanning Tree operational on the Switch. If the Countdown timer has expired and yet the Packet Storm continues, the port will be placed in Shutdown Rest mode. The port will be recovered after 5 minutes, or the user manually resets the port using the **Port Configuration** window in the **Configuration** folder. The user has to disable and enable the port for it to return to the Enabled status. Choosing this option obligates the user to configure the Interval setting as well, which will provide packet count samplings from the Switch's chip to determine if a Packet Storm is occurring.
Count Down (0 or 5-30)	The Count Down timer is set to determine the amount of time, in minutes, that the Switch will wait before shutting down the port that is experiencing a traffic storm. Only the switch continues to experience a traffic storm during this countdown period and the switch will shutdown the port. This parameter is only useful for ports configured as Shutdown in their Action field and therefore will not operate for Hardware based Traffic Control implementations. The possible time settings for this field are *0*, *5* to *30* minutes. Zero means that the port will not enter shutdown rest mode.
Time Interval (5-30)	The Interval will set the time between Multicast and Broadcast packet counts sent from the Switch's chip to the Traffic Control function. These packet counts are the determining factor in deciding when incoming packets exceed the Threshold value. The Interval may be set between *5* and *30* seconds with the default setting of *5* seconds.
Threshold (64- 1000000)	This value represents the upper threshold at which the specified traffic control is switched on. The threshold value is measured in Kbit/sec when the action is set to drop mode; it is measured in pps(packets/sec) when the action is set to shutdown mode. That is, the number of broadcast/multicast/Unknown unicast packets, received by the Switch that will trigger the storm traffic control measures. The configurable threshold range is from 64 to 1000000 with a default setting of 64. Actual rate = |rate entered/ minimum granularity|* minimal granularity, for example: 64=|100/64|*64
Storm Control Type	Select the type of Storm Type to detect: *Broadcast*, *Multicast*, *Unknown Unicast, Broadcast + Multicast*, *Broadcast + Unknown Unicast*, *Multicast + Unknown Unicast*, *Broadcast + Multicast + Unknown Unicast*, or *None*. Once selected, use the pull-down menu to enable or disable this storm detection.

Click on the **Apply** button to accept the changes made.

NOTE

Traffic Control cannot be implemented on ports that are set for Link Aggregation (Port Trunking).

NOTE

Ports that are in the Shutdown rest mode will be seen as Discarding in Spanning Tree windows and implementations though these ports will still be forwarding BPDUs to the Switch's CPU.

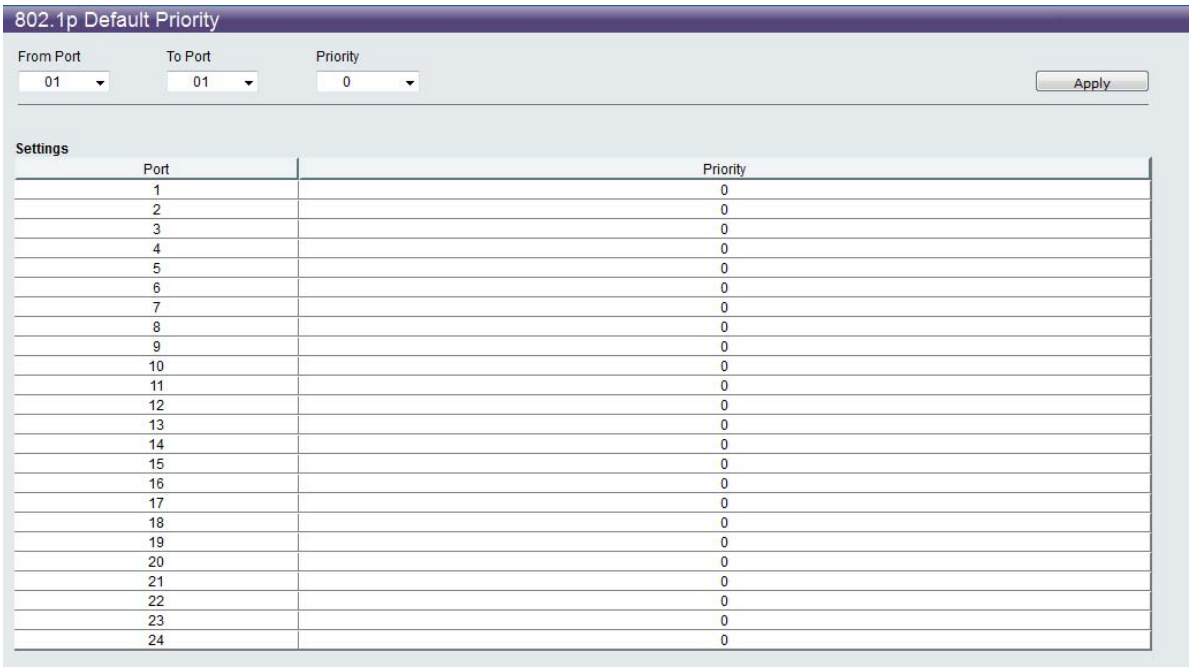
NOTE

Ports that are in Shutdown rest mode will be seen as link down in all windows and screens until the user recovers these ports or when the port automatically recover after 5 minutes.

802.1p Default Priority

The Switch allows the assignment of a default 802.1p priority to each port on the Switch.

To view this window, click **QoS > 802.1p Default Priority**:



In this window, the following parameters can be configured:

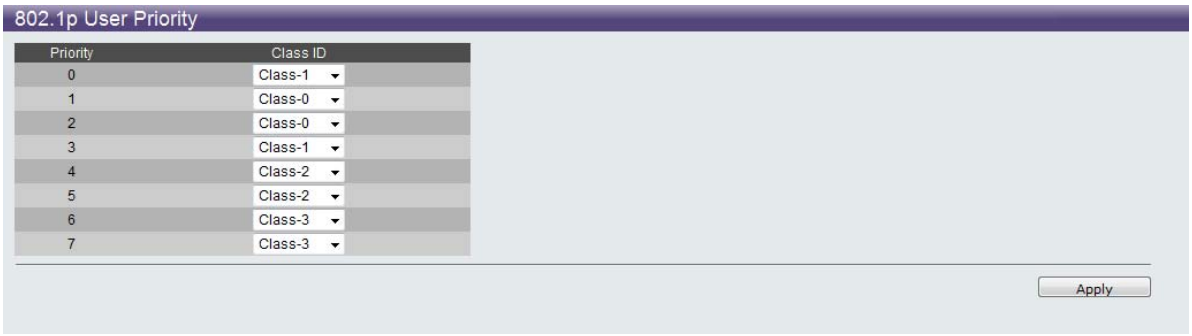
Parameter	Description
From Port/To Port	Specifies the list of ports used for this configuration
Priority	Specifies the 802.1p default priority value used.

Click on the **Apply** button to accept the changes made.

802.1p User Priority

The Switch allows the assignment of a user priority to each of the 802.1p priorities.

To view this window, click **QoS > 802.1p User Priority**:



Once a priority has been assigned to the port groups on the Switch, assign this Class to each of the eight levels of 802.1p priorities.

In this window, the following parameters can be configured:

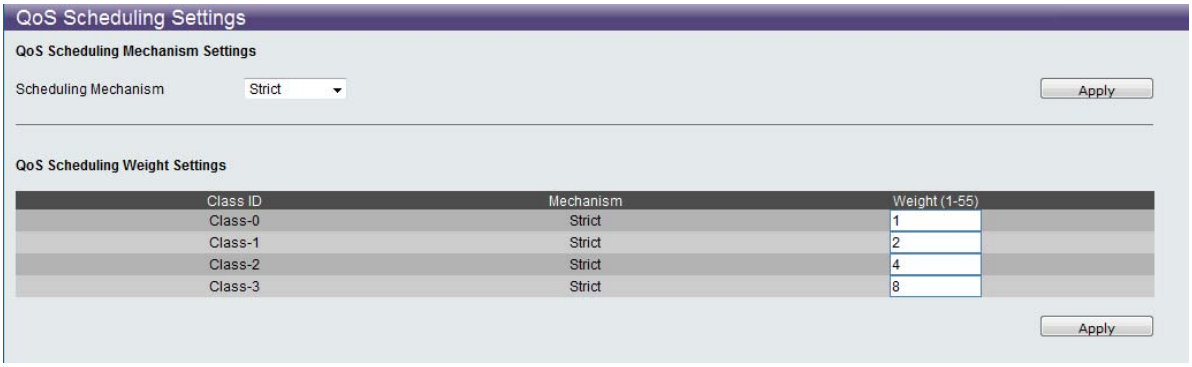
Parameter	Description
Class ID	This field is used to enter a Class ID between *Class-0* and *Class-3*.

Click on the **Apply** button to accept the changes made.

QoS Scheduling Settings

Changing the output scheduling used for the hardware queues in the Switch can customize QoS. As with any changes to QoS implementation, careful consideration should be given to how network traffic in lower priority queues are affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delays. If you choose to customize this setting, it is important to monitor network performance, especially during peak demand, as bottlenecks can quickly develop if the QoS settings are not suitable.

To view this window, click **QoS > QoS Scheduling Settings**:



In this window, the following parameters can be configured:

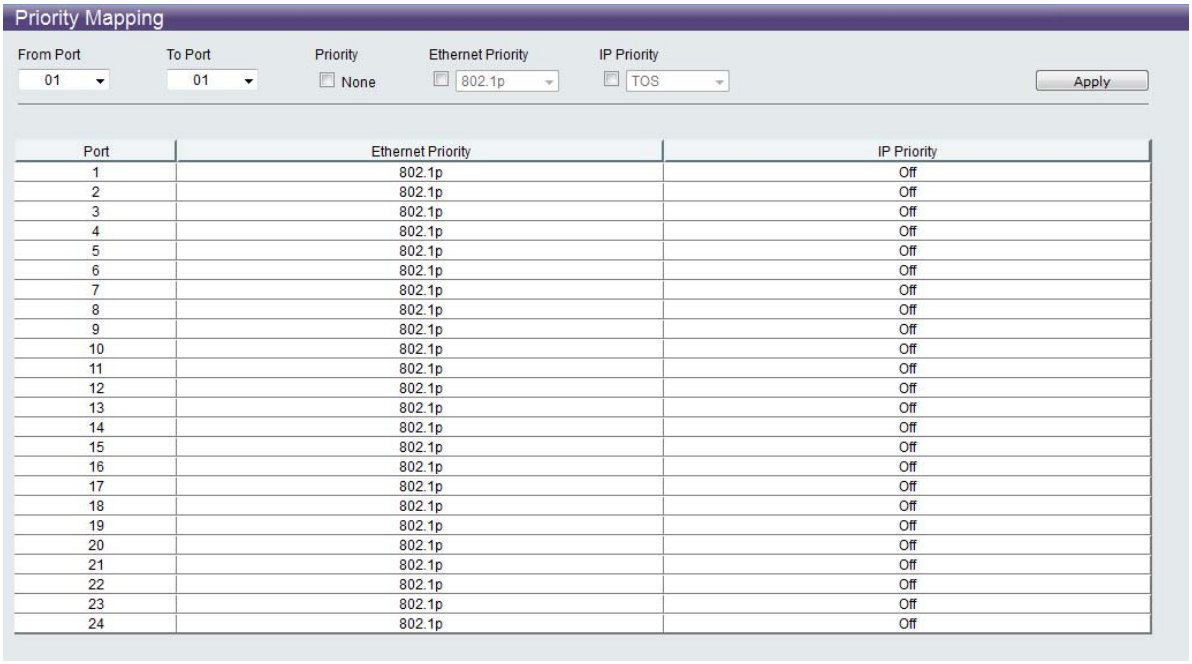
Parameter	Description
Scheduling Mechanism	Toggle between *Strict* and *Weight Fair*. *Strict* is the highest class of service and the first to process traffic. That is, the highest class of service will finish before other queues empty. *Weight Fair* uses the weighted round-robin algorithm to handle packets in an even distribution in priority classes of service.
Weight (1-55)	Enter a Weight value between *1* and *55*.

Click on the **Apply** button to accept the changes made.

Priority Mapping

This window is used to set up Priority Mapping.

To view this window, click **QoS > Priority Mapping**:



In this window, the following parameters can be configured:

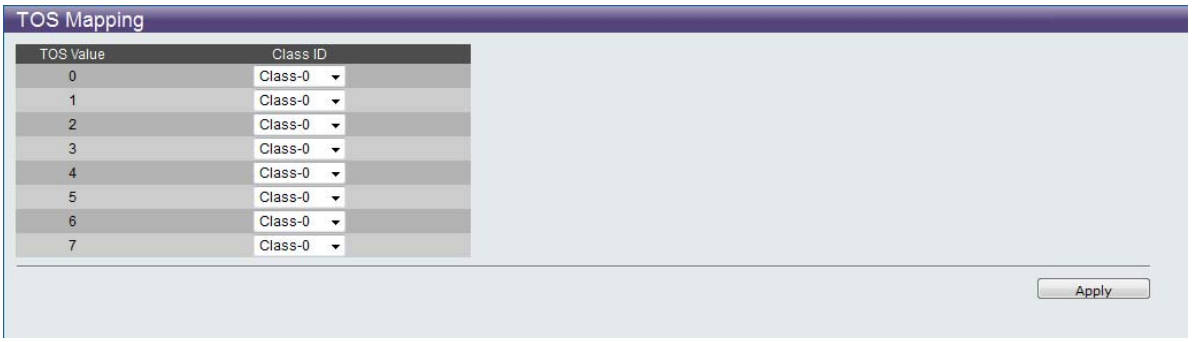
Parameter	Description
From Port/To Port	Select a range of ports to configure.
Priority	Tick the None check box neither Ethernet nor IP Priority mapping is desired.
Ethernet Priority	Tick the Ethernet Priority check box to set up 802.1p mapping.
IP Priority	Tick the IP Priority check box and then use the drop-down menu to select either *TOS* or *DSCP* mapping.

Click on the **Apply** button to accept the changes made.

TOS Mapping

This window is used to set up Type of Service (TOS) Mapping.

To view this window, click **QoS > ToS Mapping**:



In this window, the following parameters can be configured:

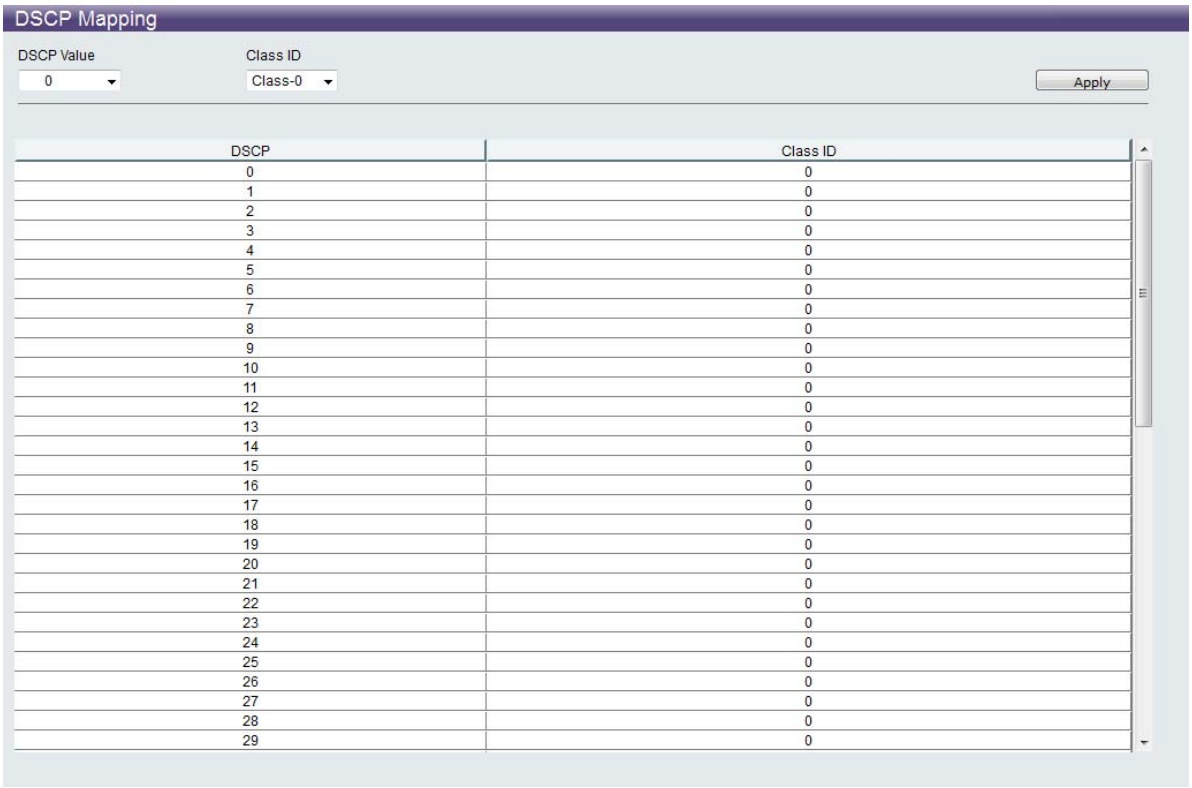
Parameter	Description
Class ID	This field is used to enter a Class ID between *Class-0* and *Class-3*.

Click on the **Apply** button to accept the changes made.

DSCP Mapping

This window is used to set up DSCP Mapping.

To view this window, click **QoS > DSCP Mapping**:



In this window, the following parameters can be configured:

Parameter	Description
DSCP Value	This field is used to enter a DSCP value in the space provided, which will instruct the Switch to examine the DiffServ Code part of each packet header and use this as the main, or part of, the criterion for forwarding. The user may choose a value between *0* and *63*.
Class ID	This field is used to enter a Class ID between *Class-0* and *Class-3*.

Click on the **Apply** button to accept the changes made.

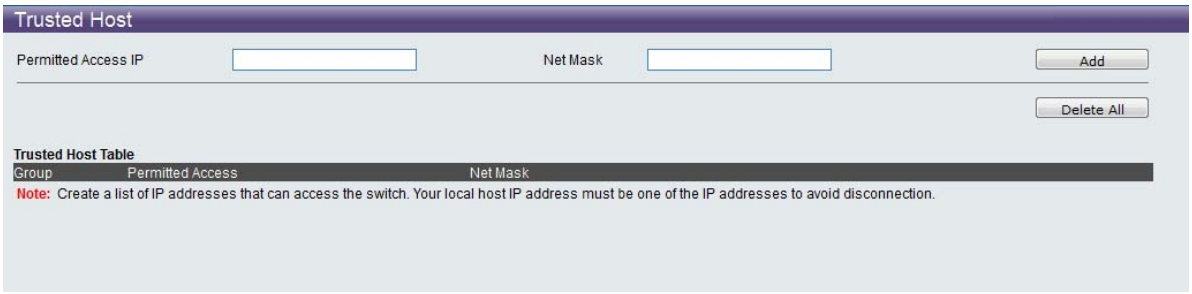
5 Security

CHAPTER

Trusted Host

Use the Security IP Management to permit remote stations to manage the Switch. If one or more designated management stations are defined by the user, only the chosen stations, as defined by the IP address and subnet, will be allowed management privilege through the Web manager, Telnet session, or SNMP manager. To define a management station IP setting, type in the IP address with a proper subnet mask and click the **Add** button.

To view this window, click **Security > Trusted Host**:


Trusted Host
Permitted Access IP
Net Mask
Add
Delete All
Trusted Host Table
Group
Permitted Access
Net Mask
Note: Create a list of IP addresses that can access the switch. Your local host IP address must be one of the IP addresses to avoid disconnection.

In this window, the following parameters can be configured:

Parameters	Description
Permitted Access IP	Specifies the trusted host permitted access IP address value used here.
Net Mask	Specifies the trusted host subnet used here.

Click on the **Add** button to add a new entry.

Click on the **Delete All** button to remove all the entries.

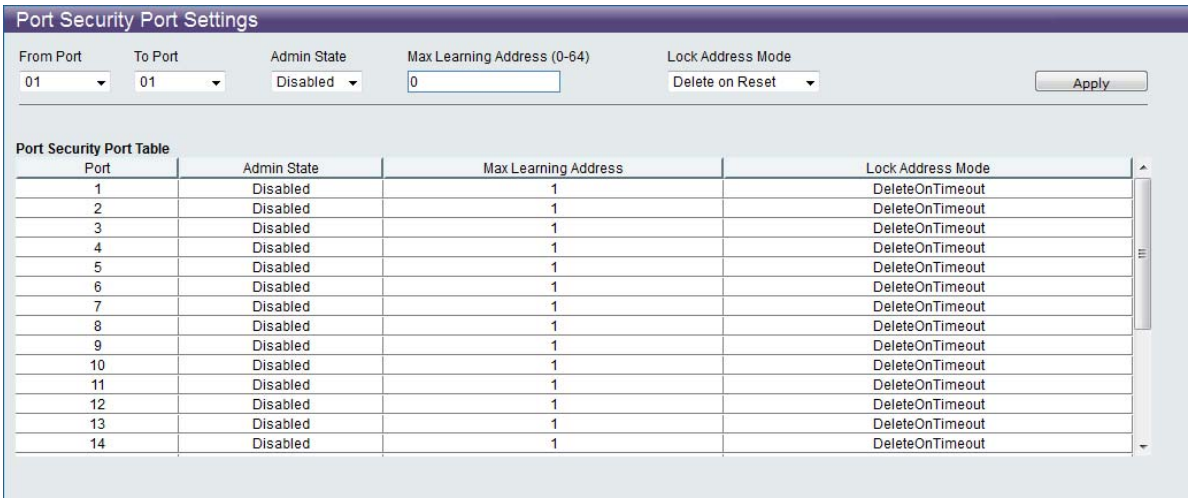
Port Security Folder

Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to locking the port (or ports) from connecting to the Switch's locked ports and gaining access to the network.

Port Security Port Settings

A given ports' (or a range of ports') dynamic MAC address learning can be locked such that the current source MAC addresses entered into the MAC address forwarding table can not be changed once the port lock is enabled. Setting the Admin State pull-down menu to *Enabled*, and clicking **Apply** can lock the port.

To view the following window, click, **Security > Port Security > Port Security Port Settings**:



In this window, the following parameters can be configured:

Parameters	Description
From Port/To Port	A consecutive group of ports may be configured starting with the selected port.
Admin State	This pull-down menu allows you to enable or disable Port Security (locked MAC address table for the selected ports).
Max. Learning Address (0-64)	The number of MAC addresses that will be in the MAC address-forwarding table for the selected switch and group of ports.
Lock Address Mode	This pull-down menu allows you to select how the MAC address table locking will be implemented on the Switch, for the selected group of ports. The options are: *Permanent* – The locked addresses will not age out after the aging timer expires. *Delete on Timeout* – The locked addresses will age out after the aging timer expires. *Delete on Reset* – The locked addresses will not age out until the Switch has been reset.

Click on the **Apply** button to accept the changes made.

Port Security FDB Entries

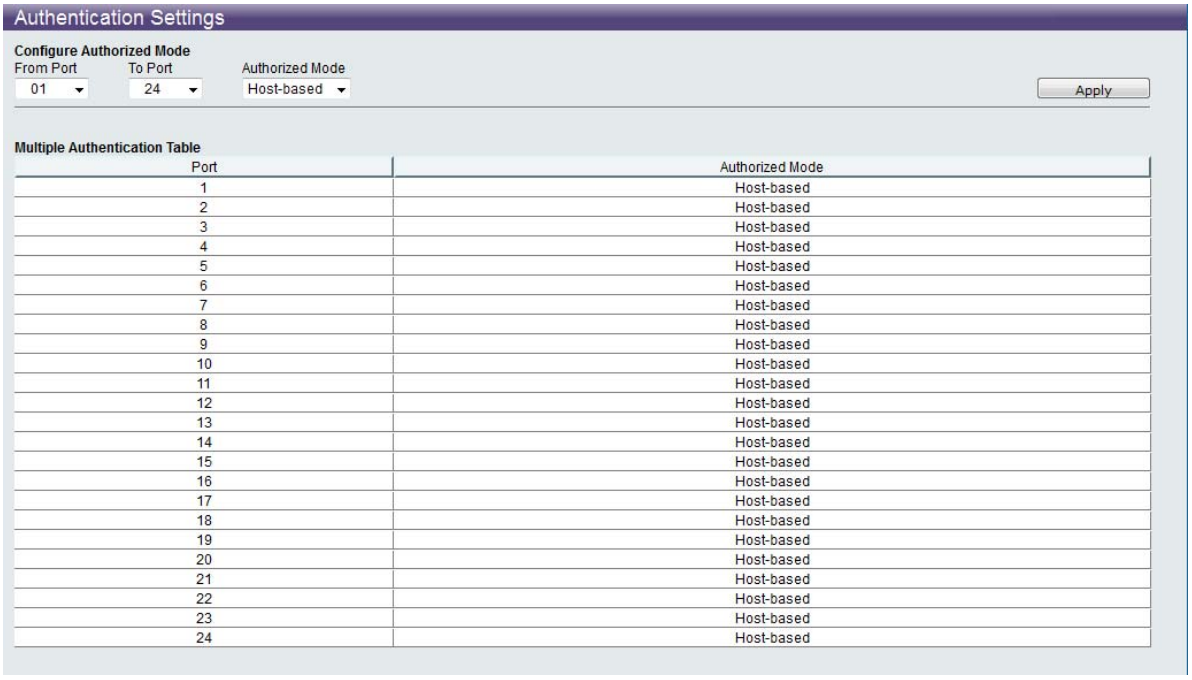
This window is used to clear the Port Lock Entries by individual ports. To clear entries enter the range of ports and click **Clear**.

To view the following window click, **Security > Port Security > Port Security FDB Entries:**

Authentication Settings

The user can use this page to configure authorization mode on ports. If the device supports multiple authentications, the port will be operated based on the authentication mode configured by the multiple authentication command.

To view this window, click **Security > Authentication Settings**:



In this window, the following parameters can be configured:

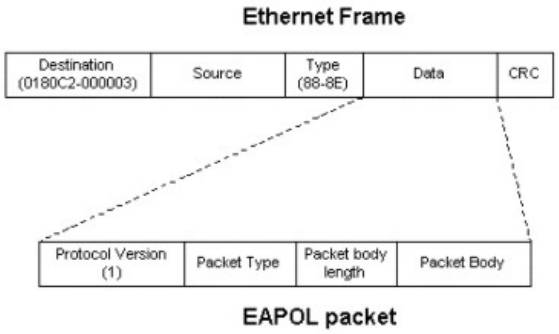
Parameters	Description
From Port ~ To Port	Here will be displayed the list of ports used for this configuration. This list is fixed on using all the ports.
Authorized Mode	Specifies the authentication mode used. *Host-based* - Every user can be authenticated individually. *Port-based* - If one of the attached hosts passes the authentication, all hosts on the same port will be granted to access network. If the user fails to authorize, this port will keep trying the next authentication. The default value is host-based.

Click on the **Apply** button to accept the changes made.

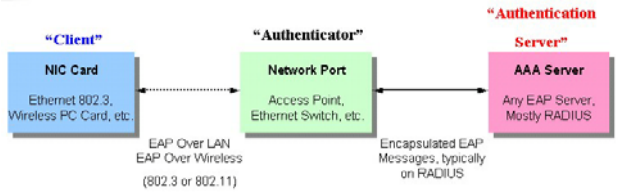
802.1X Folder

802.1X (Port-Based and Host-Based Access Control)

The IEEE 802.1X standard is a security measure for authorizing and authenticating users to gain access to various wired or wireless devices on a specified Local Area Network by using a Client and Server based access control model. This is accomplished by using a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the Client and the Server. The following figure represents a basic EAPOL packet:



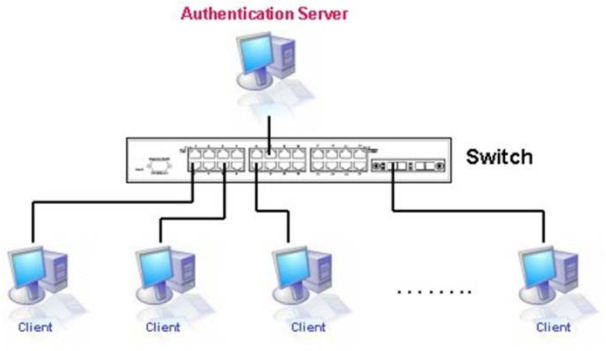
Utilizing this method, unauthorized devices are restricted from connecting to a LAN through a port to which the user is connected. EAPOL packets are the only traffic that can be transmitted through the specific port until authorization is granted. The 802.1X Access Control method has three roles, each of which are vital to creating and up keeping a stable and working Access Control security method.



The following section will explain the three roles of Client, Authenticator and Authentication Server in greater detail.

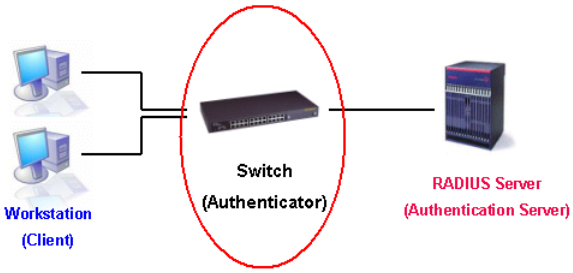
Authentication Server

The Authentication Server is a remote device that is connected to the same network as the Client and Authenticator, must be running a RADIUS Server program and must be configured properly on the Authenticator (Switch). Clients connected to a port on the Switch must be authenticated by the Authentication Server (RADIUS) before attaining any services offered by the Switch on the LAN. The role of the Authentication Server is to certify the identity of the Client attempting to access the network by exchanging secure information between the RADIUS server and the Client through EAPOL packets and, in turn, informs the Switch whether or not the Client is granted access to the LAN and/or switches services.



Authenticator

The Authenticator (the Switch) is an intermediary between the Authentication Server and the Client. The Authenticator serves two purposes when utilizing the 802.1X function. The first purpose is to request certification information from the Client through EAPOL packets, which is the only information allowed to pass through the Authenticator before access is granted to the Client. The second purpose of the Authenticator is to verify the information gathered from the Client with the Authentication Server, and to then relay that information back to the Client.



Three steps must be implemented on the Switch to properly configure the Authenticator.

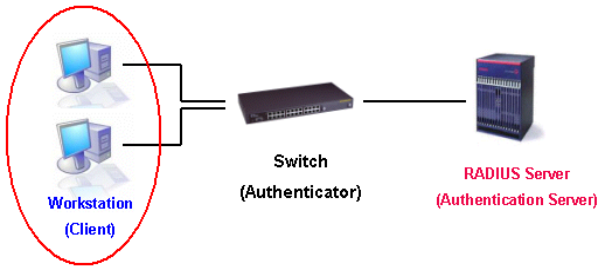
1 The 802.1X State must be *Enabled*. (**Security / 802.1X /802.1X Settings**)

2 The 802.1X settings must be implemented by port (**Security / 802.1X / 802.1X Settings**)

3 A RADIUS server must be configured on the Switch. (**Security / 802.1X / Authentic RADIUS Server**)

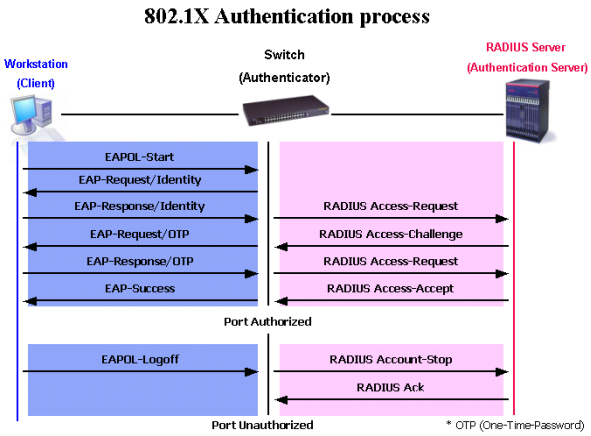
Client

The Client is simply the end station that wishes to gain access to the LAN or switch services. All end stations must be running software that is compliant with the 802.1X protocol. For users running Windows XP and Windows Vista, that software is included within the operating system. All other users are required to attain 802.1X client software from an outside source. The Client will request access to the LAN or Switch through EAPOL packets and, in turn will respond to requests from the Switch.



Authentication Process

Utilizing the three roles stated above, the 802.1X protocol provides a stable and secure way of authorizing and authenticating users attempting to access the network. Only EAPOL traffic is allowed to pass through the specified port before a successful authentication is made. This port is "locked" until the point when a Client with the correct username and password (and MAC address if 802.1X is enabled by MAC address) is granted access and therefore successfully "unlocks" the port. Once unlocked, normal traffic is allowed to pass through the port. The following figure displays a more detailed explanation of how the authentication process is completed between the three roles stated above.



The implementation of 802.1X allows network administrators to choose between two types of Access Control used on the Switch, which are:

1 Port-Based Access Control – This method requires only one user to be authenticated per port by a remote RADIUS server to allow the remaining users on the same port access to the network.

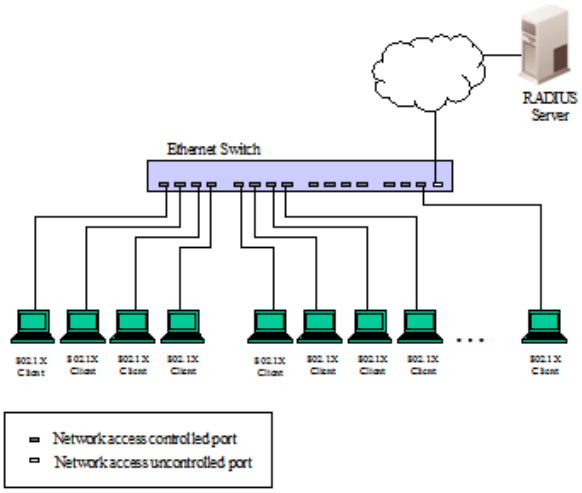
2 Host-Based Access Control – Using this method, the Switch will automatically learn up to a maximum of 16 MAC addresses by port and set them in a list. Each MAC address must be authenticated by the Switch using a remote RADIUS server before being allowed access to the Network.

Understanding 802.1X Port-based and Host-based Network Access Control

The original intent behind the development of 802.1X was to leverage the characteristics of point-to-point in LANs. As any single LAN segment in such infrastructures has no more than two devices attached to it, one of which is a Bridge Port. The Bridge Port detects events that indicate the attachment of an active device at the remote end of the link, or an active device becoming inactive. These events can be used to control the authorization state of the Port and initiate the process of authenticating the attached device if the Port is unauthorized. This is the Port-Based Network Access Control.

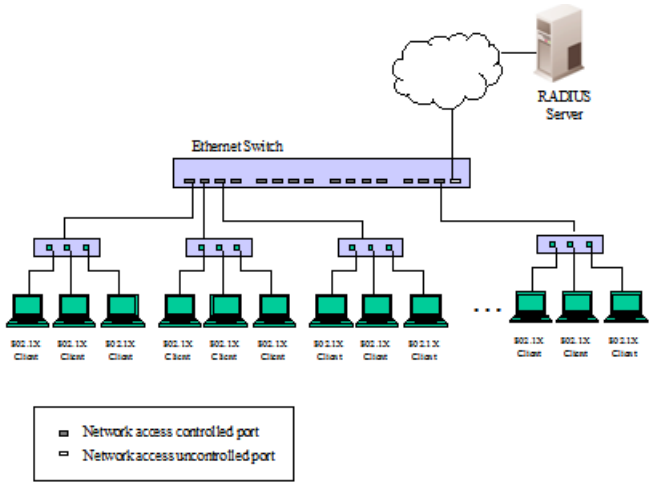
Port-Based Network Access Control

Once the connected device has successfully been authenticated, the Port then becomes Authorized, and all subsequent traffic on the Port is not subject to access control restriction until an event occurs that causes the Port to become Unauthorized. Hence, if the Port is actually connected to a shared media LAN segment with more than one attached device, successfully authenticating one of the attached devices effectively provides access to the LAN for all devices on the shared segment. Clearly, the security offered in this situation is open to attack.



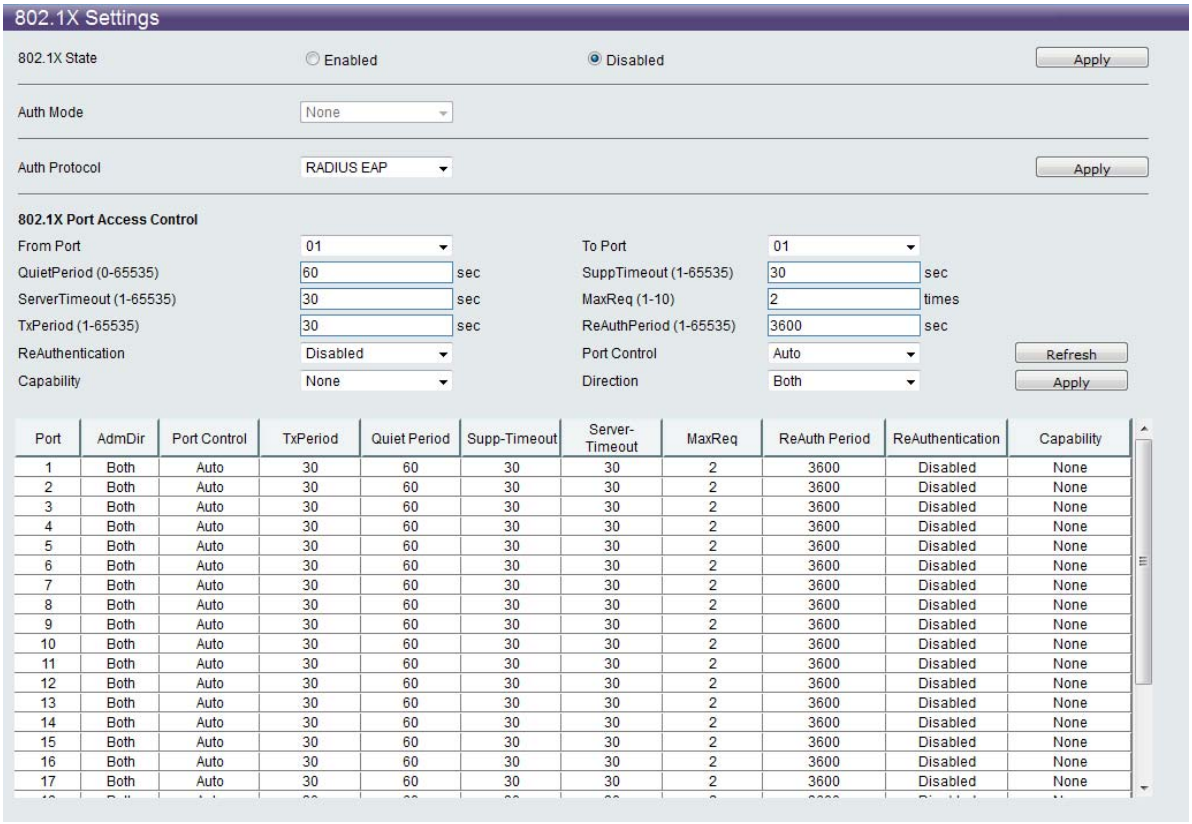
Host-Based Network Access Control

In order to successfully make use of 802.1X in a shared media LAN segment, it would be necessary to create “logical” Ports, one for each attached device that required access to the LAN. The Switch would regard the single physical Port connecting it to the shared media segment as consisting of a number of distinct logical Ports, each logical Port being independently controlled from the point of view of EAPOL exchanges and authorization state. The Switch learns each attached devices’ individual MAC addresses, and effectively creates a logical Port that the attached device can then use to communicate with the LAN via the Switch.



802.1X Settings

To configure the 802.1X Settings, click **Security > 802.1X > 802.1X Settings**:


802.1X Settings
802.1X State
Enabled
Disabled
Apply
Auth Mode
None
Auth Protocol
RADIUS EAP
Apply
802.1X Port Access Control
From Port
01
To Port
01
QuietPeriod (0-65535)
60
sec
SuppTimeout (1-65535)
30
sec
ServerTimeout (1-65535)
30
sec
MaxReq (1-10)
2
times
TxPeriod (1-65535)
30
sec
ReAuthPeriod (1-65535)
3600
sec
ReAuthentication
Disabled
Port Control
Auto
Refresh
Capability
None
Direction
Both
Apply
Port AdmDir Port Control TxPeriod Quiet Period Supp-Timeout Server-Timeout MaxReq ReAuth Period ReAuthentication Capability
1 Both Auto 30 60 30 30 2 3600 Disabled None
2 Both Auto 30 60 30 30 2 3600 Disabled None
3 Both Auto 30 60 30 30 2 3600 Disabled None
4 Both Auto 30 60 30 30 2 3600 Disabled None
5 Both Auto 30 60 30 30 2 3600 Disabled None
6 Both Auto 30 60 30 30 2 3600 Disabled None
7 Both Auto 30 60 30 30 2 3600 Disabled None
8 Both Auto 30 60 30 30 2 3600 Disabled None
9 Both Auto 30 60 30 30 2 3600 Disabled None
10 Both Auto 30 60 30 30 2 3600 Disabled None
11 Both Auto 30 60 30 30 2 3600 Disabled None
12 Both Auto 30 60 30 30 2 3600 Disabled None
13 Both Auto 30 60 30 30 2 3600 Disabled None
14 Both Auto 30 60 30 30 2 3600 Disabled None
15 Both Auto 30 60 30 30 2 3600 Disabled None
16 Both Auto 30 60 30 30 2 3600 Disabled None
17 Both Auto 30 60 30 30 2 3600 Disabled None

In this window, the following parameters can be configured:

Parameters	Description
802.1X	Use the radio buttons to enable or disable 802.1X.
Auth Mode	Here is authentication mode used will be displayed.
Auth Protocol	Choose the authentication protocol, *Local* or *RADIUS EAP.*
From Port/To Port	Enter the port or ports to be set.
QuietPeriod (0-65535)	This allows you to set the number of seconds that the Switch remains in the quiet state following a failed authentication exchange with the client. The default setting is *60* seconds.
SuppTimeout (1-65535)	This value determines timeout conditions in the exchanges between the Authenticator and the client. The default setting is *30* seconds.
ServerTimeout (1-65535)	This value determines timeout conditions in the exchanges between the Authenticator and the authentication server. The default setting is *30* seconds.
MaxReq (1-10)	The maximum number of times that the Switch will retransmit an EAP Request to the client before it times out of the authentication sessions. The default setting is *2*.
TxPeriod (1-65535)	This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. The default setting is *30* seconds.

Parameters	Description
ReAuthPeriod (1-65535)	A constant that defines a nonzero number of seconds between periodic reauthentication of the client. The default setting is *3600* seconds.
ReAuthentication	Determines whether regular reauthentication will take place on this port. The default setting is *Disabled*.
Port Control	This allows you to control the port authorization state. Select *ForceAuthorized* to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client. If *ForceUnauthorized* is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface. If *Auto* is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server. The default setting is *Auto*.
Capability	This allows the 802.1X Authenticator settings to be applied on a per-port basis. Select *Authenticator* to apply the settings to the port. When the setting is activated A user must pass the authentication process to gain access to the network. Select *None* disable 802.1X functions on the port.
Direction	Sets the administrative-controlled direction to either *in* or *both*. If *In* is selected, control is only exerted over incoming traffic through the port you selected in the first field. If *Both* are selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field.

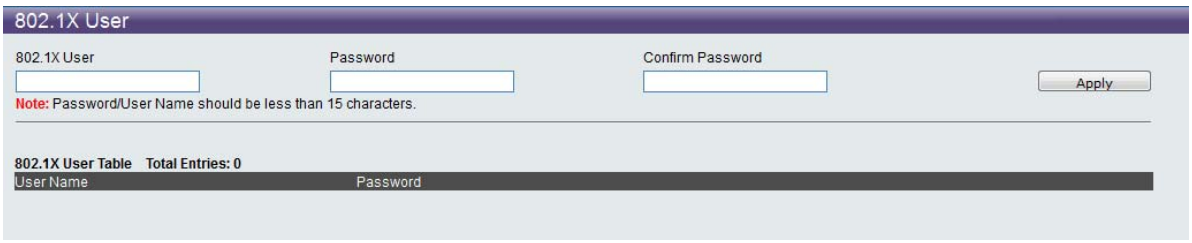
Click on the **Apply** button to accept the changes made.

Click on the **Refresh** button to refresh the display list.

802.1X User

This window is used to configure the 802.1X user settings.

To configure the 802.1X User, click **Security > 802.1X > 802.1X User**:



In this window, the following parameters can be configured:

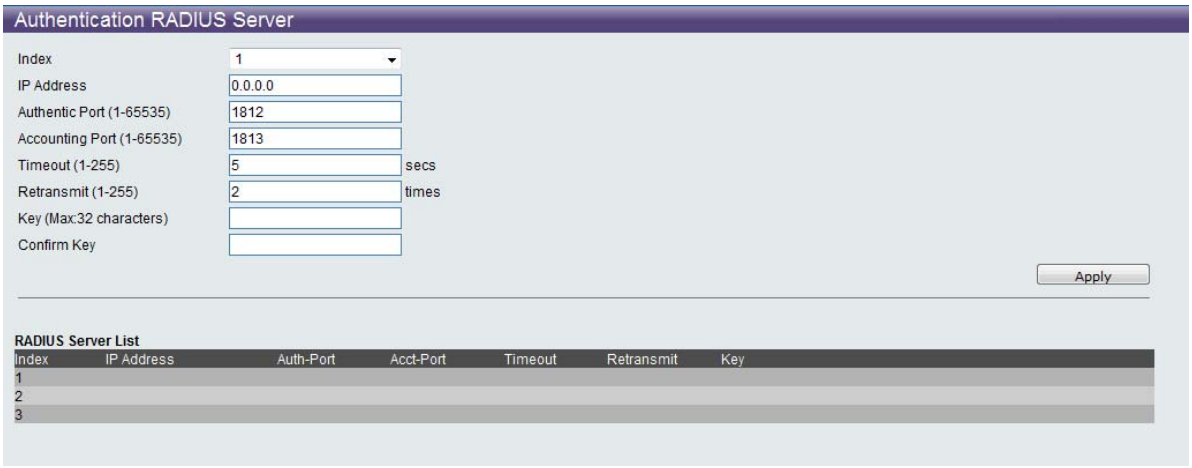
Parameters	Description
802.1X User	Specifies the 802.1X username used here.
Password	Specifies the 802.1X password used here.
Confirm Password	Specifies the 802.1X password confirmation used here.

Click on the **Apply** button to accept the changes made.

Authentication RADIUS Server

The RADIUS feature of the Switch allows you to facilitate centralized user administration as well as providing protection against a sniffing, active hacker.

To configure the 802.1X User, click **Security > 802.1X > Authentication RADIUS Server**:



In this window, the following parameters can be configured:

Parameters	Description
Index	Choose the desired RADIUS server to configure: *1*, *2* or *3*.
IP Address	Set the RADIUS Server IP.
Authentic Port (1-65535)	Set the RADIUS authentic server(s) UDP port. The default port is *1812*.
Accounting Port (1-65535)	Set the RADIUS account server(s) UDP port. The default port is *1813*.
Timeout (1-255)	Enter the timeout value in seconds (*1* to *255*) the default value is *5*.
Retransmit (1-255)	Set the retransmit value in seconds (*1* to *255*) the default value is *2*.
Key (Max. length 32 bytes)	Set the key the same as that of the RADIUS server. Maximum length of the entry is 32 bytes.

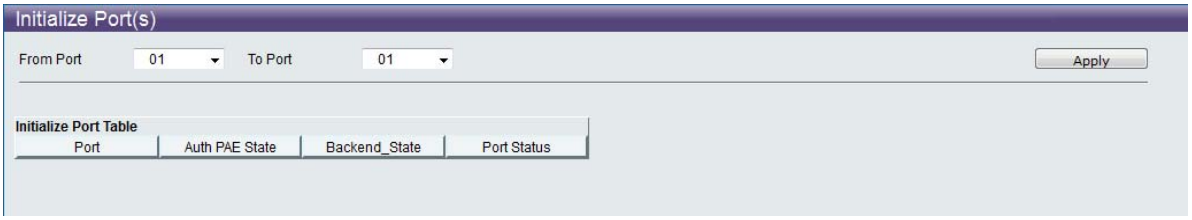
Click on the **Apply** button to accept the changes made.

Initialize Port(s)

Existing 802.1X port and MAC-based settings are displayed and can be configured using the two windows below.

To initialize ports for the port side of 802.1X, the user must first enable 802.1X by port in the **802.1X Settings** window.

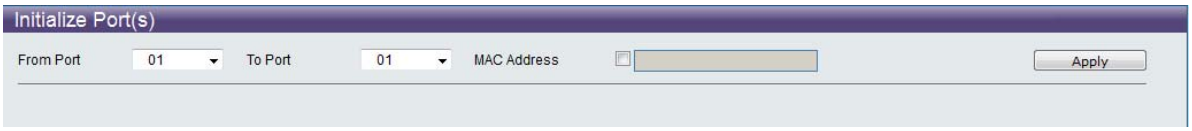
To view the following window, click **Security > 802.1X > Initialize Port(s)**:



This window allows initialization of a port or group of ports. The Initialize Port Table in the bottom half of the window displays the current status of the port(s). To initialize ports, choose the range of ports in the From Port and To Port fields. To begin the initialization, click **Apply**.

To initialize ports for the MAC-based side of 802.1X, the user must first enable 802.1X by MAC address in the **802.1X Settings** window.

To view the following window, click **Security > 802.1X > Initialize Port(s)**:



To initialize ports, choose the range of ports in the From Port and To Port fields. Next, the user must specify the MAC address to be initialized by entering it into the MAC Address field and ticking the corresponding check box. To begin the initialization, click **Apply**.

NOTE

The user must first globally enable 802.1X in the **802.1X Settings** window (**Security** > **802.1X** > **802.1X Settings**) before initializing ports. Information in the **Initialize Port(s)** windows cannot be viewed before enabling 802.1X for either Port-based 802.1X or MAC-based 802.1X.

The **Initalize Port(s)** windows display the following information:

Parameters	Description
From Port	The beginning port in a range of ports to be initialized.
To Port	The ending port in a range of ports to be initialized.
Port	A read-only field indicating a port on the Switch.
Auth PAE State	The Authenticator PAE State will display one of the following: *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth,* and *N/A.*
Backend_State	The Backend Authentication State will display one of the following: *Request, Response, Success, Fail, Timeout, Idle, Initialize,* and *N/A.*

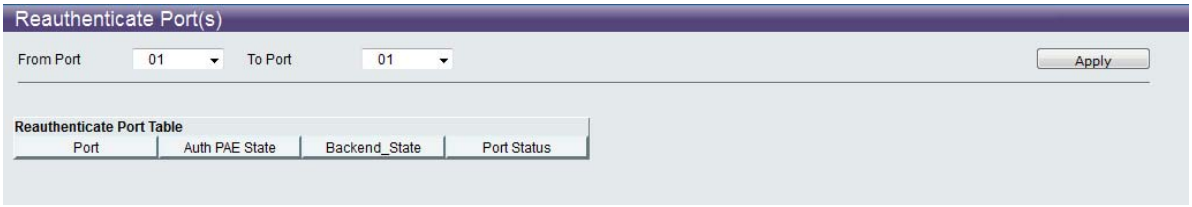
Parameters	Description
Port Status	The status of the controlled port can be *Authorized, Unauthorized*, or *N/A*.
MAC Address	The authenticated MAC address of the client connected to the corresponding port, if any.

Reauthenticate Port(s)

Users can display and configure reauthenticate ports for 802.1X port and MAC-based using the two windows below.

To reauthenticate ports for the port side of 802.1X, the user must first enable 802.1X by port in the **802.1X Settings** window

To view the following window, click **Security > 802.1X > Reauthenticate Port(s)**:



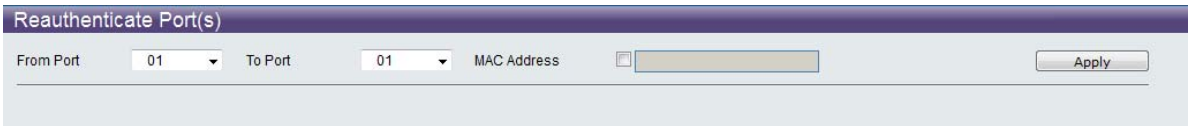
This window allows reauthentication of a port or group of ports by using the drop-down menus From Port and To Port and clicking **Apply**. The Reauthenticate Port Table displays the current status of the reauthenticated port(s) once **Apply** has been clicked.

NOTE

The user must first globally enable 802.1X in the **802.1X Settings** window (**Security** > **802.1X** > **802.1X Settings**) before reauthenticating ports. Information in the **Reauthenticate Port(s)** window cannot be viewed before enabling 802.1X.

To reauthenticate ports for the MAC-based side of 802.1X, the user must first enable 802.1X by MAC address in the **802.1X Settings** window.

To view the following window, click **Security > 802.1X > Reauthenticate Port(s)**:



To reauthenticate ports, first use the From Port and To Port drop-down menus to choose the range of ports. Then the user must specify the MAC address to be reauthenticated by entering it into the MAC Address field and ticking the corresponding check box. To begin the reauthentication, click **Apply**.

This window displays the following information:

Parameters	Description
From Port	The beginning port in a range of ports to be reauthenticated.
To Port	The ending port in a range of ports to be reauthenticated.

Parameters	Description
MAC Address	Displays the physical address of the Switch where the port resides.
Auth PAE State	The Authenticator State will display one of the following: *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth,* and *N/A.*
Backend_State	The Backend State will display one of the following: *Request, Response, Success, Fail, Timeout, Idle, Initialize,* and *N/A.*
Port Status	The status of the controlled port can be *Authorized, Unauthorized,* or *N/A.*

SSL Settings

Secure Sockets Layer or SSL is a security feature that will provide a secure communication path between a host and client through the use of authentication, digital signatures and encryption. These security functions are implemented through the use of a *ciphersuite*, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session and consists of three levels:

1 **Key Exchange:** The first part of the cyphersuite string specifies the public key algorithm to be used. This switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the *DHE DSS* Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and host as they "exchange keys" in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.

2 **Encryption:** The second part of the ciphersuite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:

   a Stream Ciphers – There are two types of stream ciphers on the Switch, *RC4 with 40-bit keys* and *RC4 with 128-bit keys*. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.

   b CBC Block Ciphers – CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the *3DES EDE* encryption code defined by the Data Encryption Standard (DES) to create the encrypted text.

3 **Hash Algorithm**: This part of the ciphersuite allows the user to choose a message digest function which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports two hash algorithms, *MD5* (Message Digest 5) and *SHA* (Secure Hash Algorithm).

   These three parameters are uniquely assembled in four choices on the Switch to create a three-layered encryption code for secure communication between the server and the host. The user may implement any one or combination of the ciphersuites available, yet different ciphersuites will affect the security level and the performance of the secured connection. The information included in the ciphersuites is not included with the Switch and requires downloading from a third source in a file form called a *certificate*. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server. The Switch supports SSLv3 and TLSv1. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to host.

Download Certificate

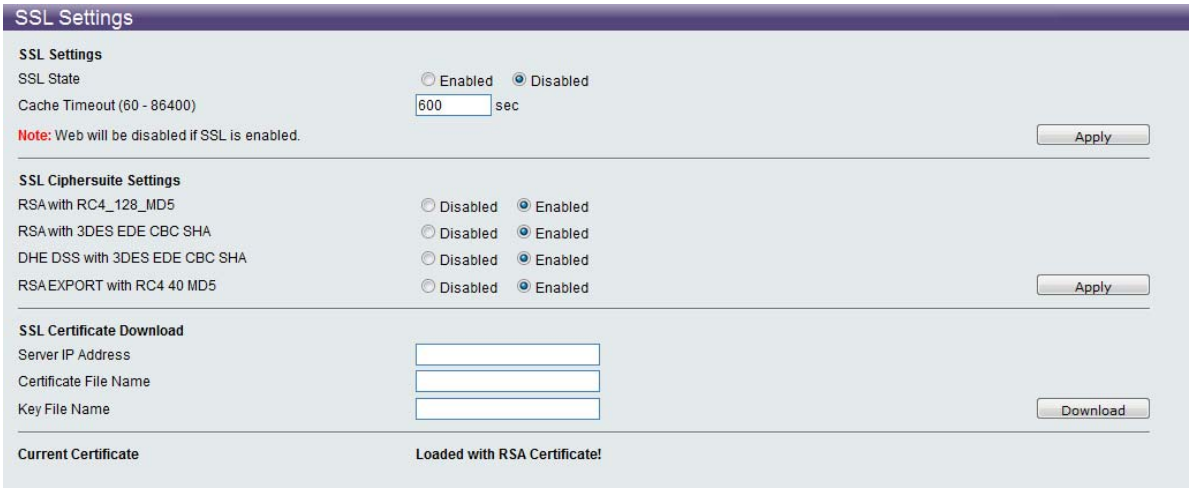
This window is used to download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. The Switch only supports certificate files with .der file extensions. The Switch is shipped with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

Ciphersuite

This window will allow the user to enable SSL on the Switch and implement any one or combination of listed ciphersuites on the Switch. A *ciphersuite* is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The Switch possesses four possible ciphersuites for the SSL function, which are all enabled by default. To utilize a particular ciphersuite, disable the unwanted ciphersuites, leaving the desired one for authentication.

When the SSL function has been enabled, the web will become disabled. To manage the Switch through the web based management while utilizing the SSL function, the web browser must support SSL encryption and the header of the URL must begin with https://. (Ex. https://10.1.1.1) Any other method will result in an error and no access can be authorized for the web-based management.

To view this window, click **Security > SSL Settings**:



In this window, the following parameters can be configured:

Parameters	Description
SSL Settings	
SSL Status	*Enable* or *Disable* the SSL status on the switch. The default is disabled.
Cache Timeout (60-86400)	This field will set the time between a new key exchange between a client and a host using the SSL function. A new SSL session is established every time the client and host go through a key exchange. Specifying a longer timeout will allow the SSL session to reuse the master key on future connections with that particular host, therefore speeding up the negotiation process. The default setting is *600* seconds.

Parameters	Description
RSA with RC4_128_MD5	This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is enabled by default.
RSA with 3DES EDE CBC SHA	This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is enabled by default.
DHE DSS with 3DES EDE CBC SHA	This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is enabled by default.
RSA EXPORT with RC4 40 MD5	This ciphersuite combines the RSA Export key exchange and stream cipher RC4 encryption with 40-bit keys. Use the pull-down menu to enable or disable this ciphersuite. This field is enabled by default.
SSL Certificate Download	
Server IP Address	Enter the IP address of the TFTP server where the certificate files are located.
Certificate File Name	Enter the path and the filename of the certificate file to download. This file must have a .der extension. (Ex. c:/cert.der)
Key File Name	Enter the path and the filename of the key file to download. This file must have a .der extension (Ex. c:/pkey.der)

Click on the **Download** button to download the SSL Certificate.

Click on the **Apply** button to accept the changes made.

NOTE

Enabling the SSL command will disable the web-based switch management. To log on to the Switch again, the header of the URL must begin with https://. Entering anything else into the address field of the web browser will result in an error and no authentication will be granted.

SSH Folder

SSH is an abbreviation of Secure Shell, which is a program allowing secure remote login and secure network services over an insecure network. It allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

The steps required to use the SSH protocol for secure communication between a remote PC (the SSH client) and the Switch (the SSH server) are as follows:

1 Create a user account with admin-level access using the User Accounts window in the **Configuration** folder. This is identical to creating any other admin-level User Account on the Switch, including specifying a password. This password is used to logon to the Switch, once a secure communication path has been established using the SSH protocol.

2 Configure the User Account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the **SSH User Authentication** window. There are three choices as to the method SSH will use to authorize the user, which are *Host Based*, *Password* and *Public Key*.

3 Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH client and the SSH server, using the **SSH Authmode and Algorithm Settings** window.

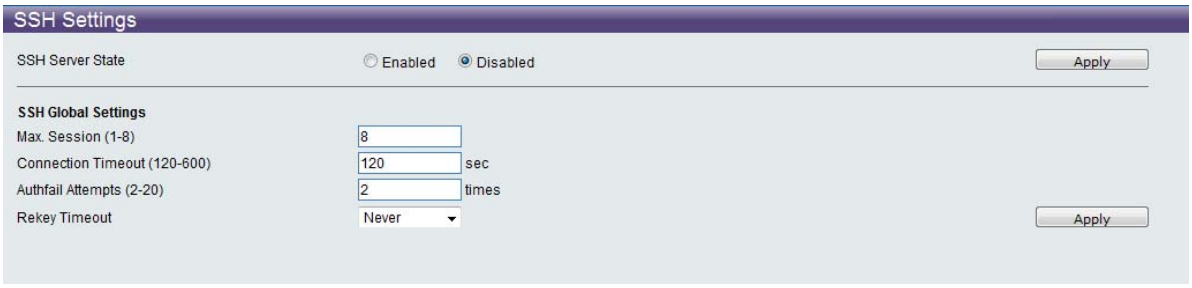
4 Finally, enable SSH on the Switch using the **SSH Settings** window.

After completing the preceding steps, a SSH Client on a remote PC can be configured to manage the Switch using a secure, in band connection.

SSH Settings

The following window is used to configure and view settings for the SSH server.

To view this window, click **Security > SSH > SSH Settings**:



In this window, the following parameters can be configured:

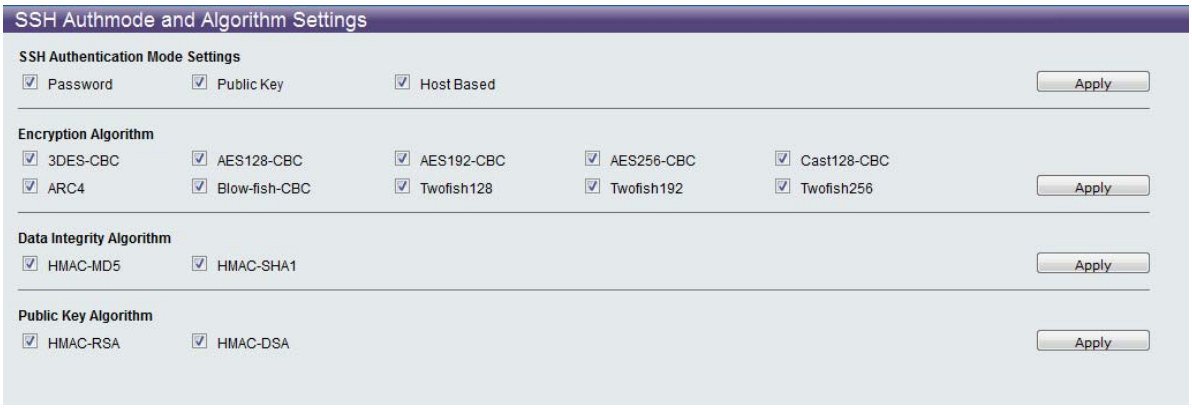
Parameters	Description
SSH Server State	Enable or disable SSH on the Switch. The default is *Disabled*.
Max Session (1-8)	Enter a value between *1* and *8* to set the number of users that may simultaneously access the Switch. The default setting is *8*.
Connection Timeout (120-600)	Allows the user to set the connection timeout. The use may set a time between *120* and *600* seconds. The default setting is *120* seconds.
Authfail Attempts (2-20)	Allows the Administrator to set the maximum number of attempts that a user may try to log on to the SSH Server utilizing the SSH authentication. After the maximum number of attempts has been exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login. The number of maximum attempts may be set between *2* and *20*. The default setting is *2*.
Rekey Timeout	Using the pull-down menu uses this field to set the time period that the Switch will change the security shell encryptions. The available options are *Never*, *10 min*, *30 min*, and *60 min*. The default setting is *Never*.

Click on the **Apply** button to accept the changes made.

SSH Authmode and Algorithm Settings

The SSH Algorithm window allows the configuration of the desired types of SSH algorithms used for authentication encryption. There are four categories of algorithms listed and specific algorithms of each may be enabled or disabled by checking the boxes. All algorithms are enabled by default.

To view this window, click **Security > SSH > SSH Authmode and Algorithm Settings:**



In this window, the following parameters can be configured:

Parameters	Description
SSH Authentication Mode Settings	
Password	This parameter may be enabled if the administrator wishes to use a locally configured password for authentication on the Switch. The default is enabled.
Public Key	This parameter may be enabled if the administrator wishes to use a public key configuration set on a SSH server, for authentication on the Switch. The default is enabled.
Host-based	This parameter may be enabled if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed. The default is enabled.
Encryption Algorithm	
3DES-CBC	Tick the check box to enable the Triple Data Encryption Standard encryption algorithm with Cipher Block Chaining. The default is enabled.
Blow-fish CBC	Tick the check box to enable the Blowfish encryption algorithm with Cipher Block Chaining. The default is enabled.
AES128-CBC	Tick the check box to enable the Advanced Encryption Standard AES128 encryption algorithm with Cipher Block Chaining. The default is enabled.
AES192-CBC	Tick the check box to enable the Advanced Encryption Standard AES192 encryption algorithm with Cipher Block Chaining. The default is enabled.
AES256-CBC	Tick the check box to enable the Advanced Encryption Standard AES-256 encryption algorithm with Cipher Block Chaining. The default is enabled.
ARC4	Tick the check box to enable the Arcfour encryption algorithm with Cipher Block Chaining. The default is enabled.
Cast128-CBC	Tick the check box to enable the Cast128 encryption algorithm with Cipher Block Chaining. The default is enabled.
Twofish128	Tick the check box to enable the twofish128 encryption algorithm. The default is enabled.
Twofish192	Tick the check box to enable the twofish192 encryption algorithm. The default is enabled.
Twofish256	Tick the check box to enable the twofish256 encryption algorithm. The default is enabled.
Data Integrity Algorithm	

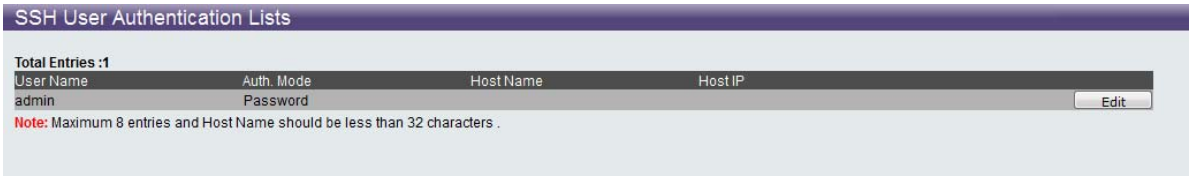
Parameters	Description
HMAC-SHA1	Tick the check box to enable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Secure Hash algorithm. The default is enabled.
HMAC-MD5	Tick the check box to enable the HMAC (Hash for Message Authentication Code) mechanism utilizing the MD5 Message Digest encryption algorithm. The default is enabled.
Public Key Algorithm	
HMAC-RSA	Tick the check box to enable the HMAC (Hash for Message Authentication Code) mechanism utilizing the RSA encryption algorithm. The default is enabled.
HMAC-DSA	Tick the check box to enable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Digital Signature Algorithm encryption. The default is enabled.

Click on the **Apply** button to accept the changes made.

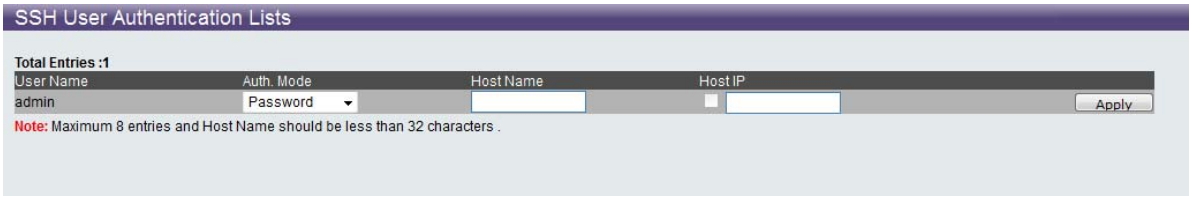
SSH User Authentication Lists

The following windows are used to configure parameters for users attempting to access the Switch through SSH.

To access the following window, click **Security > SSH > SSH User Authentication Lists**:



In the example above, the User Account "cts" has been previously set using the **User Accounts** window in the **Configuration** folder. A User Account MUST be set in order to set the parameters for the SSH user. To edit the parameters for a SSH user, click on the corresponding **Edit** button, which will reveal the following window to configure:



In this window, the following parameters can be configured:

Parameters	Description
User Name	Enter a User Name of no more than 15 characters to identify the SSH user. This User Name must be a previously configured user account on the Switch.

Parameters	Description
Auth. Mode	The administrator may choose one of the following to set the authorization for users attempting to access the Switch. *Host Based* – This parameter should be chosen if the administrator wishes to use a remote SSH server for authentication purposes. Choosing this parameter requires the user to input the following information to identify the SSH user. *Host Name* – Enter an alphanumeric string of no more than 32 characters to identify the remote SSH user. *Host IP* – Enter the corresponding IP address of the SSH user. *Password* – This parameter should be chosen if the administrator wishes to use an administrator-defined password for authentication. Upon entry of this parameter, the Switch will prompt the administrator for a password, and then to re-type the password for confirmation. *Public Key* – This parameter should be chosen if the administrator wishes to use the publickey on a SSH server for authentication.
Host Name	Enter an alphanumeric string of no more than 32 characters to identify the remote SSH user. This parameter is only used in conjunction with the Host Based choice in the Auth. Mode field.
Host IP	Enter the corresponding IP address of the SSH user. This parameter is only used in conjunction with the Host Based choice in the Auth. Mode field.

Click on the **Apply** button to accept the changes made.

NOTE

To set the SSH User Authentication parameters on the Switch, a User Account must be previously configured. For more information on configuring local User Accounts on the Switch, see the User Accounts section of this manual located in the Configuration section.

Access Authentication Control Folder

The TACACS/XTACACS/TACACS+/RADIUS commands allow users to secure access to the Switch using the TACACS/XTACACS/TACACS+/RADIUS protocols. When a user logs in to the Switch or tries to access the administrator level privilege, he or she is prompted for a password. If TACACS/XTACACS/TACACS+/RADIUS authentication is enabled on the Switch, it will contact a TACACS/XTACACS/TACACS+/RADIUS server to verify the user. If the user is verified, he or she is granted access to the Switch.

There are currently three versions of the TACACS security protocol, each a separate entity. The Switch's software supports the following versions of TACACS:

- **TACACS** (Terminal Access Controller Access Control System) - Provides password checking and authentication, and notification of user actions for security purposes utilizing via one or more centralized TACACS servers, utilizing the UDP protocol for packet transmission.
- **Extended TACACS (XTACACS)** - An extension of the TACACS protocol with the ability to provide more types of authentication requests and more types of response codes than TACACS. This protocol also uses UDP to transmit packets.

- **TACACS+ (Terminal Access Controller Access Control System plus)** - Provides detailed access control for authentication for network devices. TACACS+ is facilitated through Authentication commands via one or more centralized servers. The TACACS+ protocol encrypts all traffic between the Switch and the TACACS+ daemon, using the TCP protocol to ensure reliable delivery

In order for the TACACS/XTACACS/TACACS+/RADIUS security function to work properly, a TACACS/XTACACS/TACACS+/RADIUS server must be configured on a device other than the Switch, called an Authentication Server Host and it must include usernames and passwords for authentication. When the user is prompted by the Switch to enter usernames and passwords for authentication, the Switch contacts the TACACS/XTACACS/TACACS+/RADIUS server to verify, and the server will respond with one of three messages:

- The server verifies the username and password, and the user is granted normal user privileges on the Switch.
- The server will not accept the username and password and the user is denied access to the Switch.
- The server doesn't respond to the verification query. At this point, the Switch receives the timeout from the server and then moves to the next method of verification configured in the method list.

The Switch has four built-in Authentication Server Groups, one for each of the TACACS, XTACACS, TACACS+ and RADIUS protocols. These built-in Authentication Server Groups are used to authenticate users trying to access the Switch. The users will set Authentication Server Hosts in a preferable order in the built-in Authentication Server Groups and when a user tries to gain access to the Switch, the Switch will ask the first Authentication Server Hosts for authentication. If no authentication is made, the second server host in the list will be queried, and so on. The built-in Authentication Server Groups can only have hosts that are running the specified protocol. For example, the TACACS Authentication Server Groups can only have TACACS Authentication Server Hosts.

The administrator for the Switch may set up six different authentication techniques per user-defined method list (TACACS/XTACACS/TACACS+/RADIUS/local/none) for authentication. These techniques will be listed in an order preferable, and defined by the user for normal user authentication on the Switch, and may contain up to eight authentication techniques. When a user attempts to access the Switch, the Switch will select the first technique listed for authentication. If the first technique goes through its Authentication Server Hosts and no authentication is returned, the Switch will then go to the next technique listed in the server group for authentication, until the authentication has been verified or denied, or the list is exhausted.

Please note that when the user logins to the device successfully through TACACS/XTACACS/ TACACS+/RADIUS server or none method, the “user” priviledge level is the only level assigned. If the user wants to get the administration privilege level, the user must use the “enable admin” command to promote his privilege level.

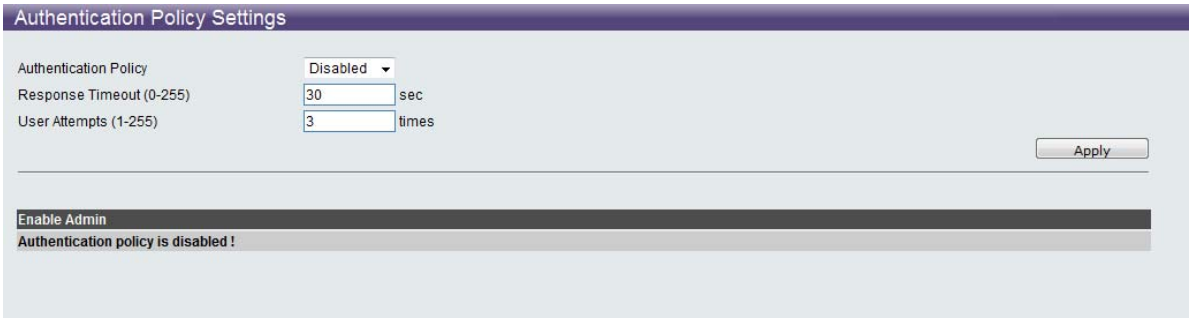
NOTE

TACACS, XTACACS and TACACS+ are separate entities and are not compatible. The Switch and the server must be configured exactly the same, using the same protocol. (For example, if the Switch is set up for TACACS authentication, so must be the host server.)

Authentication Policy Settings

This window offers an administrator-defined authentication policy for users trying to access the Switch. When *Enabled*, the device will check the Login Method List and choose a technique for user authentication upon login.

To access the following window, click **Security > Access Authentication Control > Authentication Policy Settings**:



In this window, the following parameters can be configured:

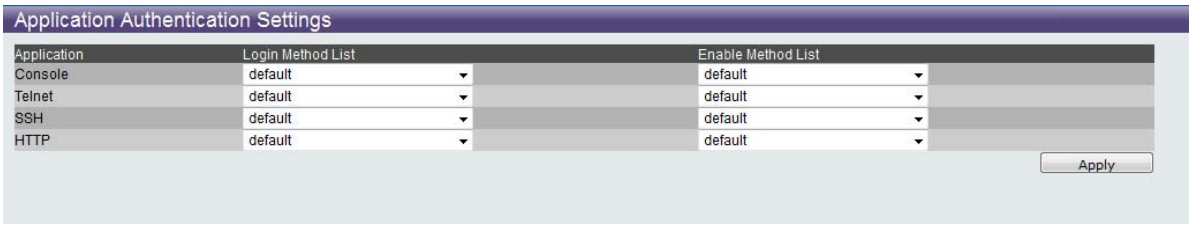
Parameters	Description
Authentication Policy	Use the pull-down menu to enable or disable the Authentication Policy on the Switch.
Response Timeout (0-255)	This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between *0* and *255* seconds. The default setting is *30* seconds.
User Attempts (1-255)	This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet and web users will be disconnected from the Switch. The user may set the number of attempts from *1* to *255*. The default setting is *3*.

Click on the **Apply** button to accept the changes made.

Application Authentication Settings

This window is used to configure switch configuration applications (console, Telnet, SSH, HTTP) for login at the user level and at the administration level (Enable Admin) utilizing a previously configured method list.

To view the following window, click **Security > Access Authentication Control > Application Authentication Settings**:



In this window, the following parameters can be configured:

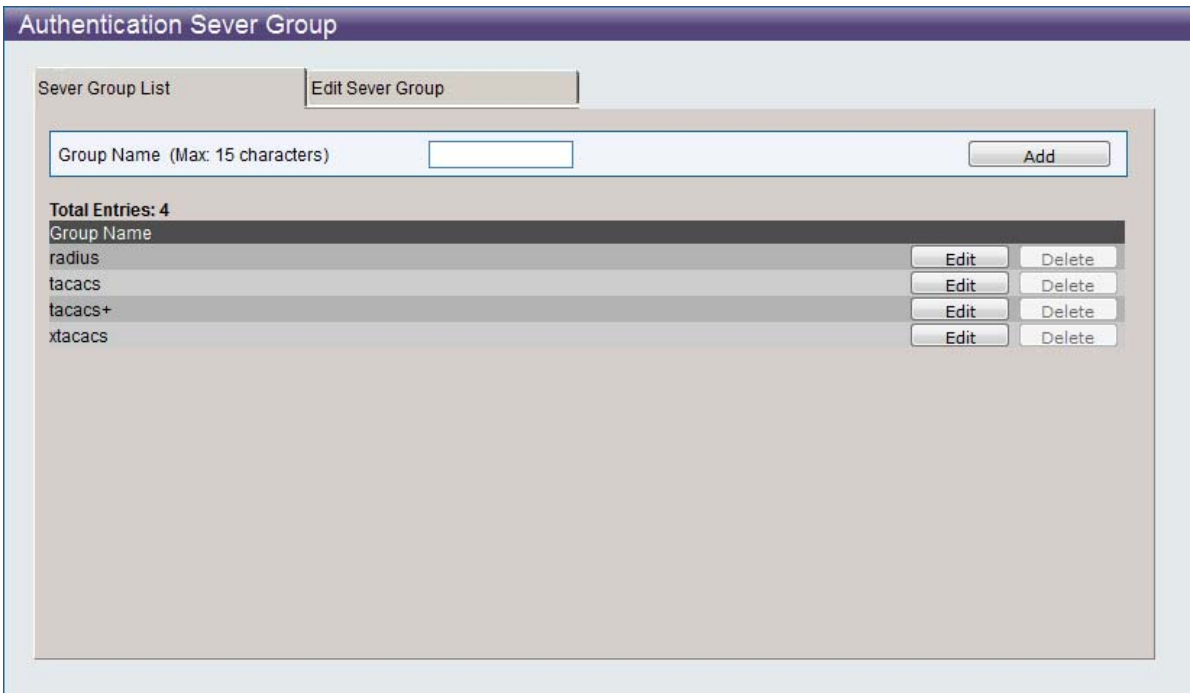
Parameters	Description
Application	Lists the configuration applications on the Switch. The user may configure the Login Method List and Enable Method List for authentication for users utilizing the Console (Command Line Interface) application, the Telnet application, SSH, and the WEB (HTTP) application.
Login Method List	Using the pull-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the **Login Method Lists** window, in this section, for more information.
Enable Method List	Using the pull-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the **Enable Method Lists** window, in this section, for more information

Click on the **Apply** button to accept the changes made.

Authentication Server Group

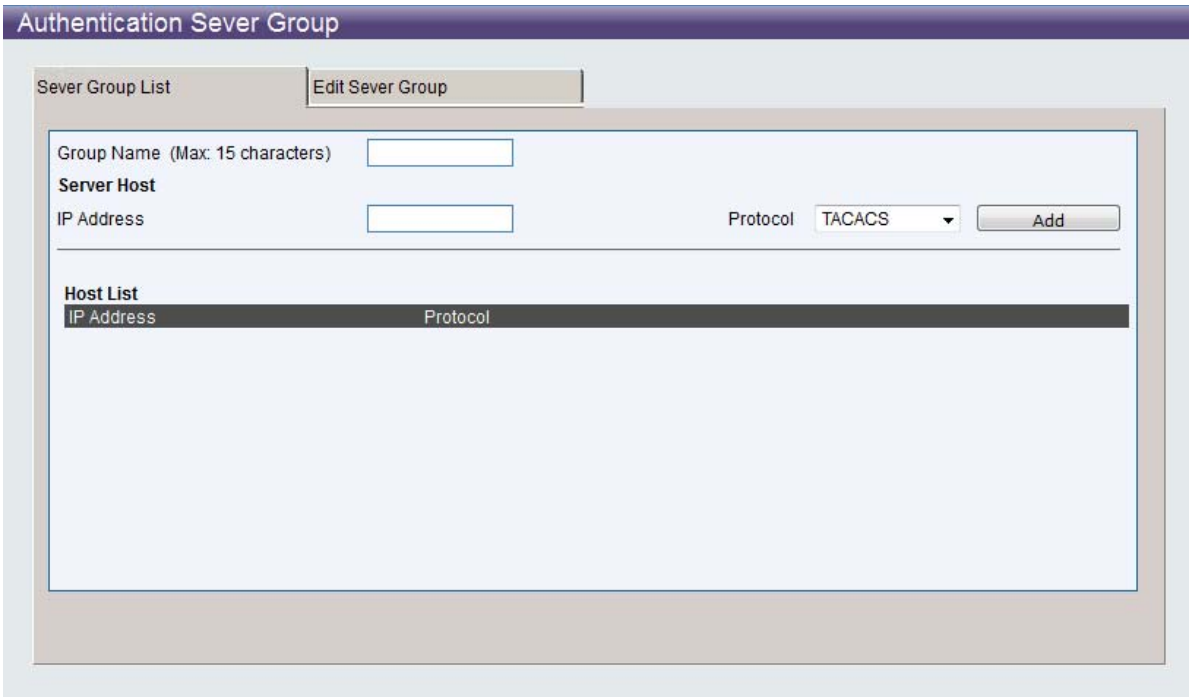
This window will allow users to set up Authentication Server Groups on the Switch. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user-defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. The Switch has three built-in Authentication Server Groups that cannot be removed but can be modified. Up to eight authentications server hosts may be added to any particular group.

To view the following window, click **Security > Access Authentication Control > Authentication Server Group**:



The Switch has four built-in Authentication Server Groups that cannot be removed but can be modified.

To modify a particular group, click on its corresponding **Edit** button or click the **Edit Server Group** tab at the top of this window, the following tab will be displayed:



To add an Authentication Server Host to the list, enter its IP address in the IP Address field, choose the protocol associated with the IP address of the Authentication Server Host and click **Add** to add this Authentication Server Host to the group.

NOTE

The user must configure Authentication Server Hosts using the Authentication Server Hosts window before adding hosts to the list. Authentication Server Hosts must be configured for their specific protocol on a remote centralized server before this function can work properly.

NOTE

The four built in server groups can only have server hosts running the same TACACS daemon. TACACS/XTACACS/TACACS+ protocols are separate entities and are not compatible with each other.

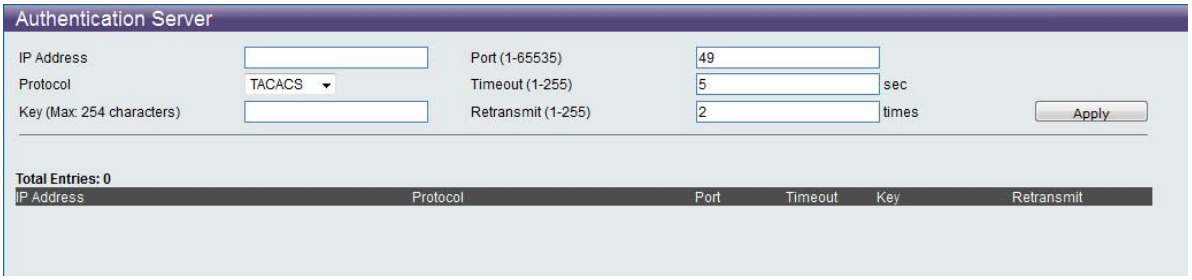
Authentication Server

This window will set user-defined Authentication Server Hosts for the TACACS/XTACACS/TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with Authentication Policy enabled, the Switch will send authentication packets to a remote TACACS/XTACACS/TACACS+/RADIUS server host on a remote host. The TACACS/XTACACS/TACACS+/RADIUS server host will then verify or deny the request and return the appropriate message to the

Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.

To view the following window, click **Security > Access Authentication Control > Authentication Server**:

In this window, the following parameters can be configured:



Parameters	Description
IP Address	The IP address of the remote server host the user wishes to add.
Port (1-65535)	Enter a number between *1* and *65535* to define the virtual port number of the authentication protocol on a server host. The default port number is *49* for TACACS/XTACACS/TACACS+ servers and *1812* for RADIUS servers but the user may set a unique port number for higher security.
Protocol	The protocol used by the server host. The user may choose one of the following: *TACACS* - Enter this parameter if the server host utilizes the TACACS protocol. *XTACACS* - Enter this parameter if the server host utilizes the XTACACS protocol. *TACACS+* - Enter this parameter if the server host utilizes the TACACS+ protocol. *RADIUS* - Enter this parameter if the server host utilizes the RADIUS protocol.
Timeout (1-255)	Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is *5* seconds.
Key	Authentication key to be shared with a configured TACACS+ or RADIUS servers only. Specify an alphanumeric string up to 254 characters.
Retransmit (1-255)	Enter the value in the retransmit field to change how many times the device will resend an authentication request when the server does not respond. The default value is 2 times.

Click on the **Apply** button to accept the changes made.

NOTE

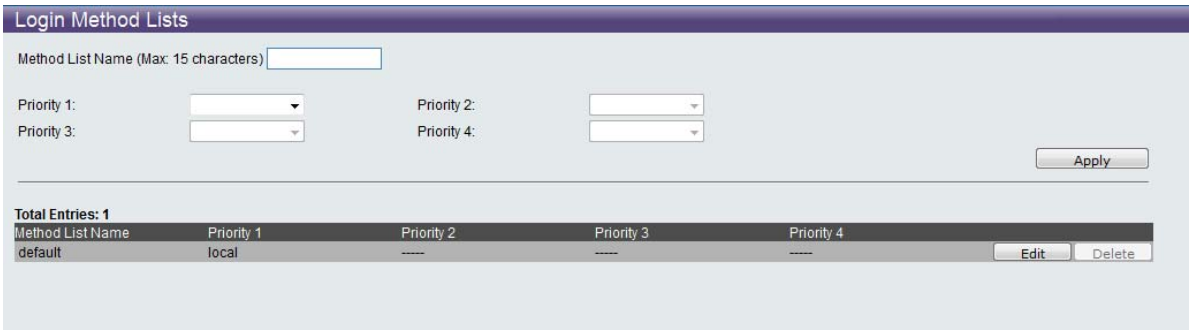
More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+ are separate entities and are not compatible with each other.

Login Method Lists

This window is used to configure a user-defined or default Login Method List of authentication techniques for users logging on to the Switch. The sequence of techniques implemented in this command will affect the authentication result. For example, if a user enters a sequence of techniques, for example TACACS – XTACACS - local, the Switch will send an authentication request to the first TACACS host in the server group. If no response comes from the server host, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the local account database set in the Switch is used to authenticate the user. When the local method is used, the privilege level will be dependant on the local account privilege configured on the Switch.

When the user logins to the device successfully through TACACS/XTACACS/TACACS+/RADIUS server or none method, the "user" privilege level is assigned only. If the user wants to get admin privilege level, the user must use the **Enable Admin** window to promote his privilege level. (See the Enable Admin part of this section for more detailed information.)

To view the following window, click **Security > Access Authentication Control > Login Method Lists:**



The Switch contains one Method List that is set and cannot be removed, yet can be modified. To delete a Login Method List defined by the user, click the corressponding **Delete** button. To modify a Login Method List, click on its corresponding **Edit** button.

In this window, the following parameters can be configured:

Parameters	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.

Parameters	Description
Priority 1, 2, 3, 4	The user may add one, or a combination of up to four of the following authentication methods to this method list: *tacacs* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. *xtacacs* - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server. *tacacs+* - Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server. *radius* - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server. *server_group* - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch. *local* - Adding this parameter will require the user to be authenticated using the local user account database on the Switch. *none* - Adding this parameter will require no authentication to access the Switch.

Click on the **Apply** button to accept the changes made.

Enable Method Lists

This window is used to set up Method Lists to promote users with user level privileges to Administrator (Admin) level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight Enable Method Lists can be implemented on the Switch, one of which is a default Enable Method List. This default Enable Method List cannot be deleted but can be configured.

The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like TACACS - XTACACS - Local Enable, the Switch will send an authentication request to the first TACACS host in the server group. If no verification is found, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the Local Enable password set in the Switch is used to authenticate the user.

Successful authentication using any of these methods will give the user an "Admin" privilege.

NOTE

To set the Local Enable Password, see the next section, entitled Local Enable Password.

To view the following table, click **Security > Access Authentication Control > Enable Method Lists:**

To delete an Enable Method List defined by the user, click the the **Delete** button. To modify an Enable Method List, click on its corresponding **Edit** button.

In this window, the following parameters can be configured:

Parameters	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.
Priority 1, 2, 3, 4	The user may add one, or a combination of up to four of the following authentication methods to this method list: *local_enable* - Adding this parameter will require the user to be authenticated using the local enable password database on the Switch. The user in the next section entitled Local Enable Password must set the local enable password. *none* - Adding this parameter will require no authentication to access the Switch. *radius* - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server. *tacacs* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. *xtacacs* - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server. *tacacs+* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. server_group - Adding a previously configured server group will require the user to be authenticated using a user-defined server group previously configured on the Switch.

Click on the **Apply** button to accept the changes made.

Local Enable Password Settings

This window will configure the locally enabled password for the **enable admin** command. When a user chooses the "local_enable" method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here that is locally set on the Switch.

To view the following window, click **Security > Access Authentication Control > Local Enable Password Settings**:

Local Enable Password Settings
Old Local Enable Password (Max: 15 characters)
New Local Enable Password
Confirm Local Enable Password
Apply

In this window, the following parameters can be configured:

Parameters	Description
Old Local Enable Password (Max: 15 characters)	If a password was previously configured for this entry, enter it here in order to change it to a new password
New Local Enable Password	Enter the new password that you wish to set on the Switch to authenticate users attempting to access Administrator Level privileges on the Switch. The user may set a password of up to 15 characters.
Confirm Local Enable Password	Confirm the new password entered above. Entering a different password here from the one set in the New Local Enabled field will result in a fail message.

Click on the **Apply** button to accept the changes made.

MAC-based Access Control Folder

MAC-based Access Control is a method to authenticate and authorize access using either a port or host. For port-based MAC, the method decides port access rights, while for host-based MAC, the method determines the MAC access rights.

A MAC user must be authenticated before being granted access to a network. Both local authentication and remote RADIUS server authentication methods are supported. In MAC-based Access Control, MAC user information in a local database or a RADIUS server database is searched for authentication. Following the authentication result, users achieve different levels of authorization.

Notes About MAC-based Access Control

There are certain limitations and regulations regarding the MAC-based Access Control:

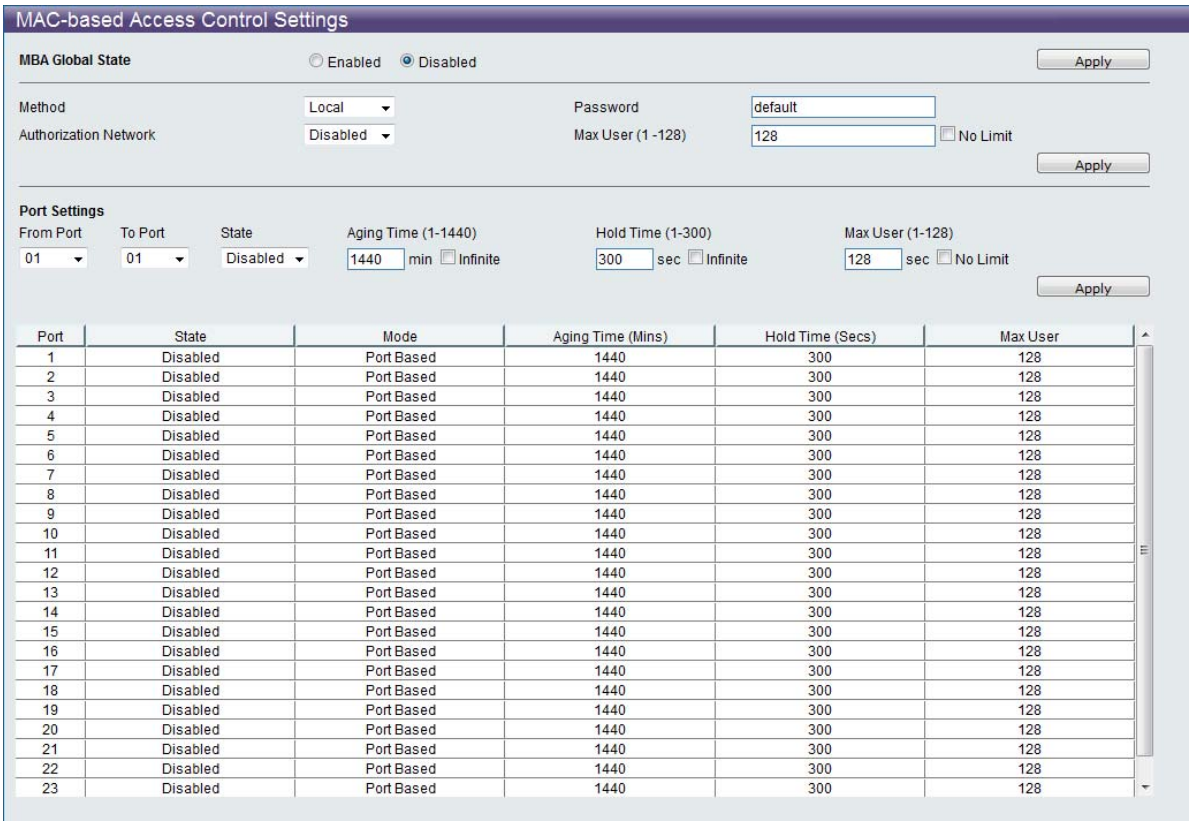
1 Once this feature is enabled for a port, the Switch will clear the FDB of that port.

2 Ports that have been enabled for Link Aggregation, Port Security, or GVRP authentication cannot be enabled for MAC-based Authentication.

MAC-based Access Control Settings

The following window is used to set the parameters for the MAC-based Access Control function on the Switch. Here the user can set the running state, method of authentication, and RADIUS password to be associated with the MAC-based Access Control function of the Switch.

To enable the MAC-based Access Control Global Settings on the Switch, click **Security > MAC-based Access Control > MAC-based Access Control Settings**:



In this window, the following parameters can be configured:

Parameters	Description
Settings	
MBA Global State	Use the radio button to globally enable or disable the MAC-based Access Control function on the Switch.
Method	Use the pull-down menu to choose the type of authentication to be used when authentication MAC addresses on a given port. The user may choose between the following methods: *Local* – Use this method to utilize the locally set MAC address database as the authenticator for MAC-based Access Control. This MAC address list can be configured in the MAC-based Access Control Local Database Settings window. *RADIUS* – Use this method to utilize a remote RADIUS server as the authenticator for MAC-based Access Control. Remember, the MAC list must be previously set on the RADIUS server and the settings for the server must be first configured on the Switch.
Password	Enter the password for the RADIUS server, which is to be used for packets being sent requesting authentication. The default password is *default*.
Max User (1–128)	Enter a value for the maximum number of users, between *1* and *128*. The default is *128*.

Parameters	Description
Authorization Network	When enabled, authorized attributes (for example VLAN) assigned by the RADUIS server or local database. Which attributes will be accepted depends on the individual module's setting. Authorization for attributes is disabled by default.

Click on the **Apply** button to accept the changes made.

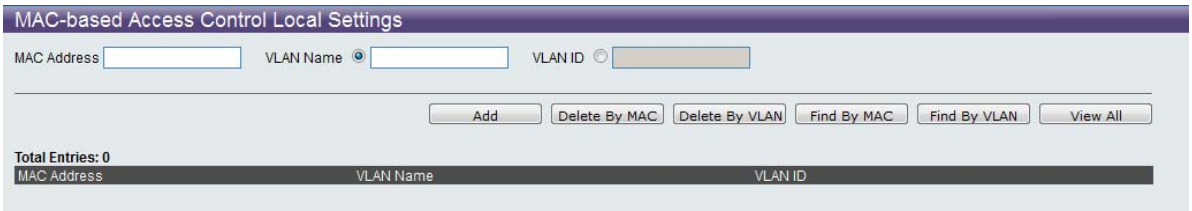
Parameters	Description
Port Settings	
From Port/To Port	Enter the Port range.
State	Use the pull-down menu to enable or disable the MAC-based Access Control function on individual ports.
Aging Time (1-1440)	Enter an aging value between *1* and *1440* minutes. The default is *1440*. Tick the Infinite check box for no aging time.
Hold Time (1-300)	Enter a hold value between *1* and *300* seconds. The default is *300*. Tick the Infinite check box for no hold time.
Max User (1-128)	Enter a value for the maximum number of users, between *1* and *128*. The default is *128*. Tick the No Limit check box for no maximum user limit.

Click on the **Apply** button to accept the changes made.

MAC-based Access Control Local Settings

The following window is used to set a list of MAC addresses, along with their corresponding target VLAN, which will be authenticated for the Switch. Once a queried MAC address is matched in this table, it will be placed in the VLAN associated with it here. The switch administrator may enter up to 128 MAC addresses to be authenticated using the local method configured here.

To enable the MAC-based Access Control Local MAC Settings on the switch, click **Security > MAC-based Access Control > MAC-based Access Control Local Settings**:



Click on the **Add** button to add a new entry.

Click on the **Delete By MAC** button to delete an entry based on the MAC address entered.

Click on the **Delete By VLAN** button to delete an entry based on the VLAN name or ID entered.

Click on the **Find By MAC** button to find an entry based on the MAC address entered.

Click on the **Find By VLAN** button to find an entry based on the VLAN name or ID entered.

Click on the **View All** button to view all the available entries on this Switch.

Click on the **Edit By Name** button to re-configure the VLAN name of the specific entry.

Click on the **Edit By ID** button to re-configure the VLAN ID of the specific entry.

6 Access Control List (ACL)

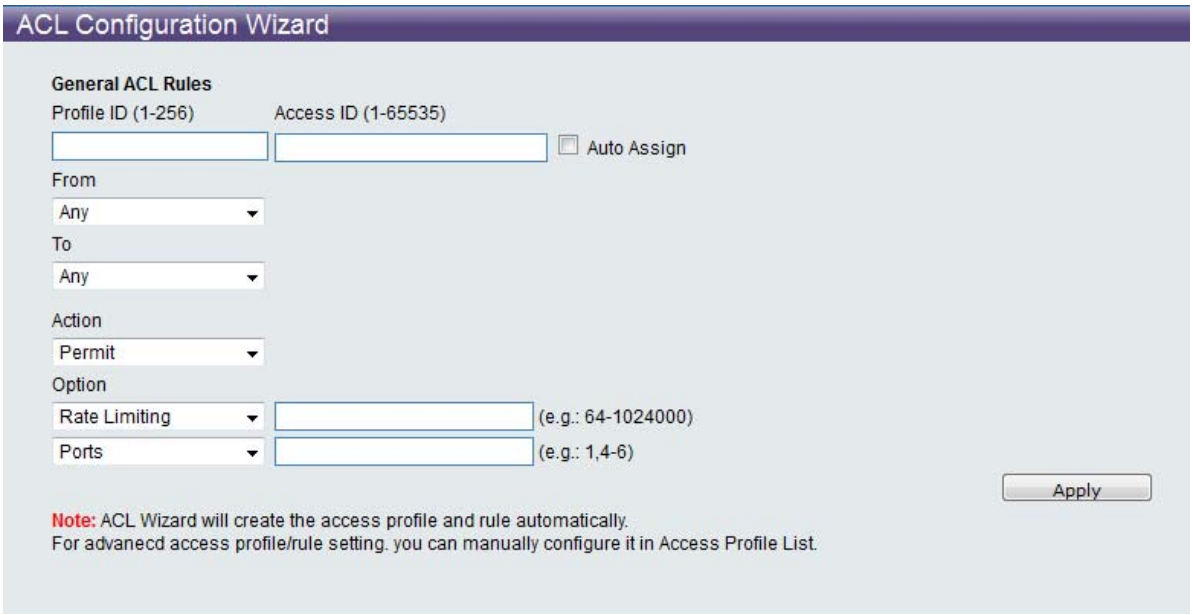
CHAPTER

Access profiles allow the user to establish criteria to determine whether or not the Switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a basis of Packet Content, MAC address, IP address, or IPv6 address.

ACL Configuration Wizard

This window will aid with the creation of access profiles and ACL Rules. The ACL Wizard will create the access rule and profile automatically.

To view this window click, **ACL > ACL Configuration Wizard:**



In this window, the following parameters can be configured:

Parameters	Description
Profile ID (1-256)	Enter a unique identifier number for this profile set. This value can be set from *1* to *256*.

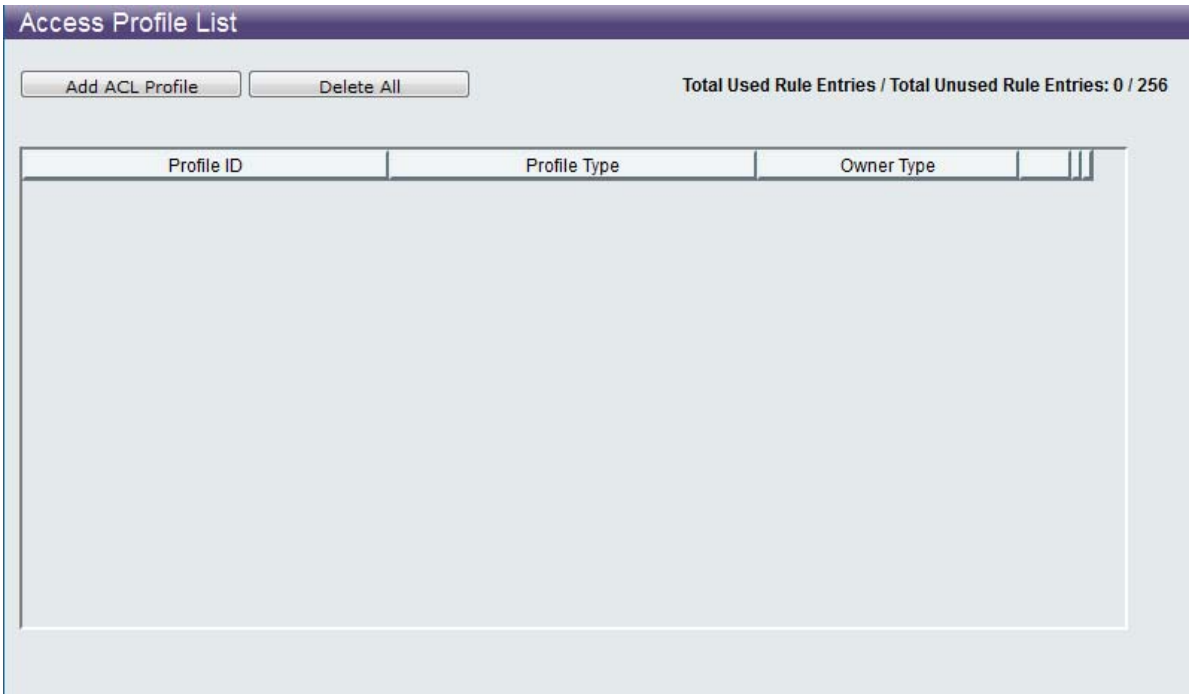
Parameters	Description
Access ID (1-65535)	Type in a unique identifier number for this access. This value can be set from *1* to *65535*.
From	Use the drop-down menu to select from *MAC Address*, *IPv4 Address*, *IPv6*, or *Any*.
To	Use the drop-down menu to select from *MAC Address*, *IPv4 Address*, or *Any*.
Service Type	Use the drop-down menu to select from *VLAN Name*, *Ethernet Type*, *802.1P*, or *Any*.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Option	Select between *Rate Limiting*, *Change 1P Priority*, and *Replace DSCP*.
Ports	Enter a range of ports to be configured.

Click on the **Apply** button to accept the changes made.

Access Profile List

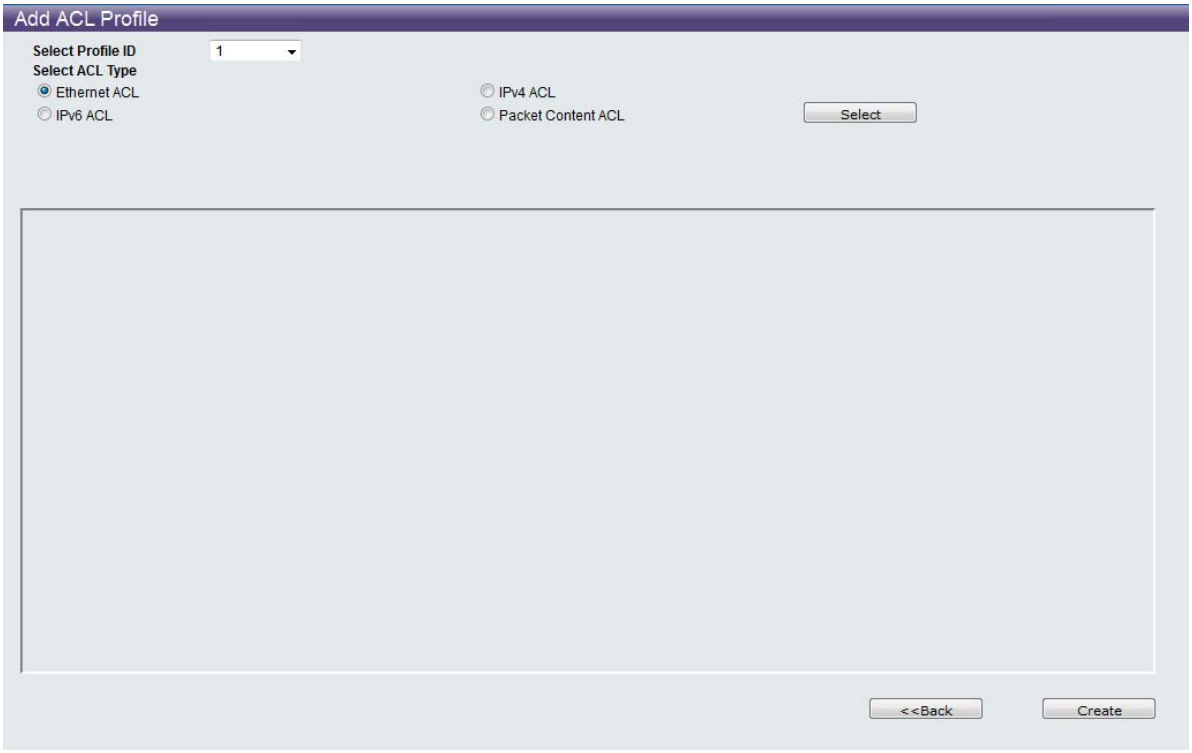
Creating an access profile is divided into two basic parts. The first is to specify which part or parts of a frame the Switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the Switch will use to determine what to do with the frame. The entire process is described below in two parts.

To display the currently configured Access Profiles on the Switch, click **ACL > Access Profile Lists**:



Access Profile List – Enternet ACL

To add an ACL Profile, click the **Add ACL Profile** button, which will display the window below:



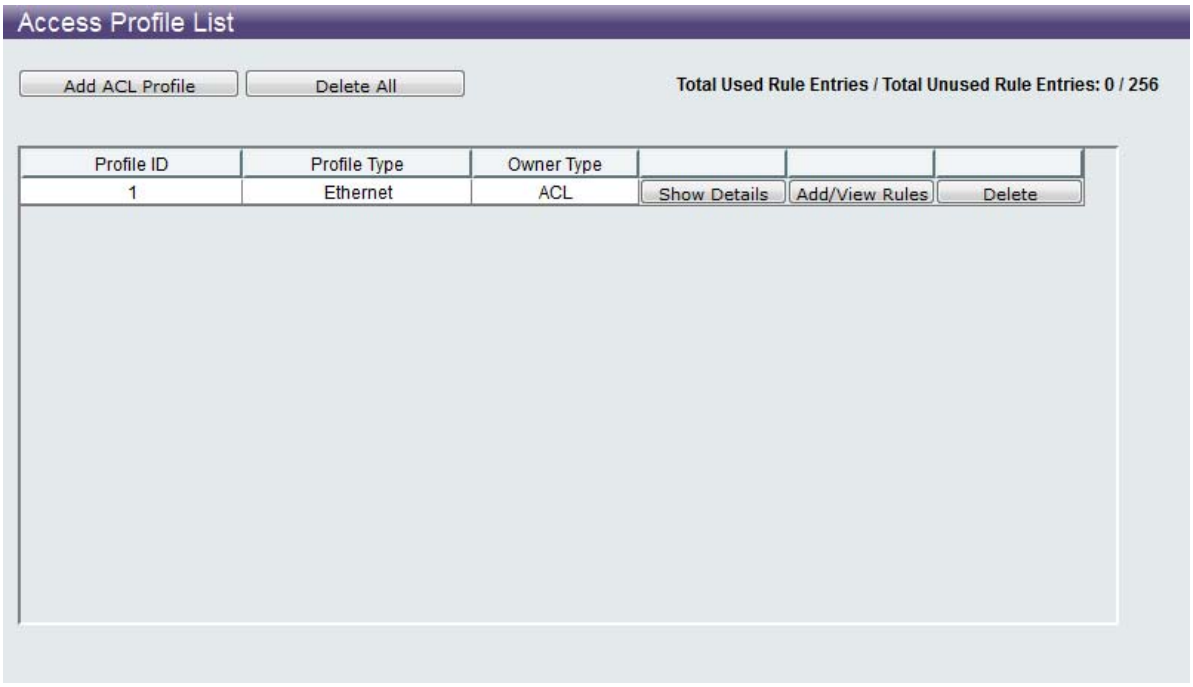
There are four sets of Access Profile configuration windows; one for Ethernet (or MAC address-based) profile configuration, one for IP (IPv4) address-based profile configuration, one for the Packet Content and one for IPv6. Explore the four types of Access Profile configuration options by using the drop-down menu to select a Profile ID between *1* and *256* (*1* has been selected in this example), using the radio button to select an ACL Type (Ethernet ACL has been selected in this example), and then clicking **Select**. Next, click on the boxes near the top of the window, which will then turn red and reveal parameters for configuration (MAC Address, 802.1Q VLAN, 802.1p, and Ethernet Type have been selected in this example). At least one mask must then be selected before clicking the **Create** button (802.1p has been ticked in this example). To return to the Access Profile List window, click **<<Back**.

In this window, the following parameters can be configured:

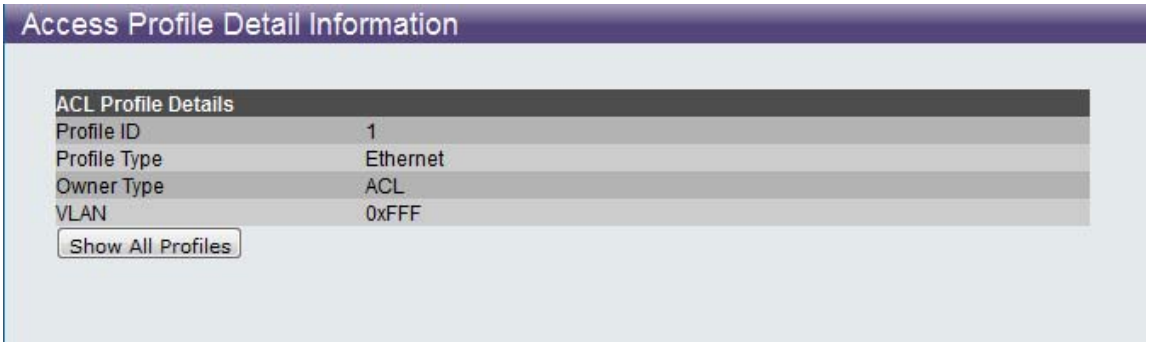
Parameters	Description
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 or packet content mask. This will change the window according to the requirements for the type of profile.
	Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header.
	Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header.
	Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header.
	Select Packet Content ACL to specify a mask to mask the content of the packet header.
MAC Address	Tick either Source MAC Mask and enter the source MAC address mask or Destination MAC Mask and enter the destination MAC address mask.
802.1Q VLAN	VLAN - Specifies a VLAN.
	VLAN Mask (0-FFF) - Specifies a VLAN mask.
	Selecting this option instructs the Switch to examine the VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
802.1p	Selecting this option instructs the Switch to examine the 802.1p priority value of each packet header and use this as the, or part of the criterion for forwarding.
Ethernet Type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

Clicking **Create** on the previous **Add ACL Profile** window inserts a new Access Profile List entry in the **Access Profile List** window shown below. To add another Access Profile, click **Add ACL Profile**. To delete a profile click the corresponding **Delete** button, to delete all the entries click on the **Delete** All button, to view the specific configurations for an entry click the **Show Details** button.

To add a rule to the Access Profile entry, click the **Add/View Rules** button.

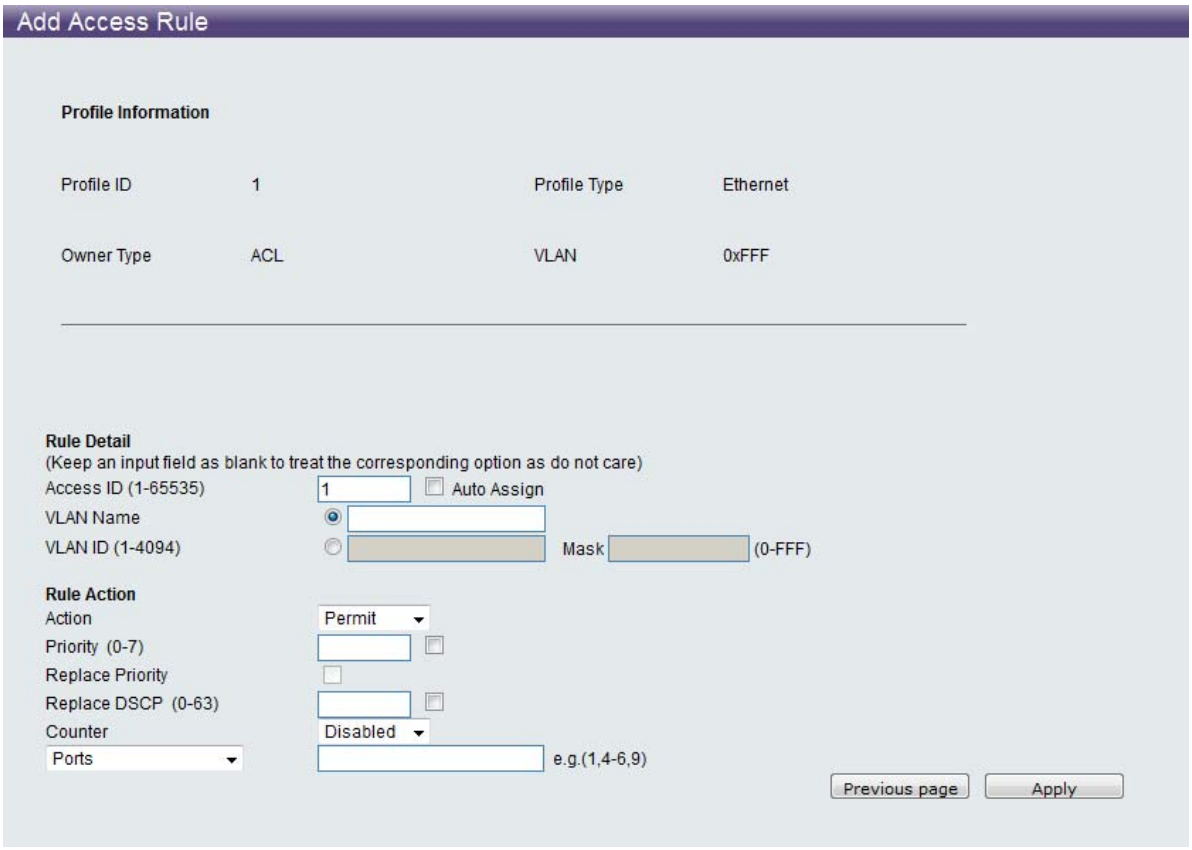


To view the configurations for a previously configured entry, click on the corresponding **Show Details** button, which will display the following window:



To return to the **Access Profile List** window, click **Show All Profiles**. To add a rule to a previously configured entry click on the corresponding **Add/View Rules**. The following window is displayed:

Click **Add Rule**, to display the following window:

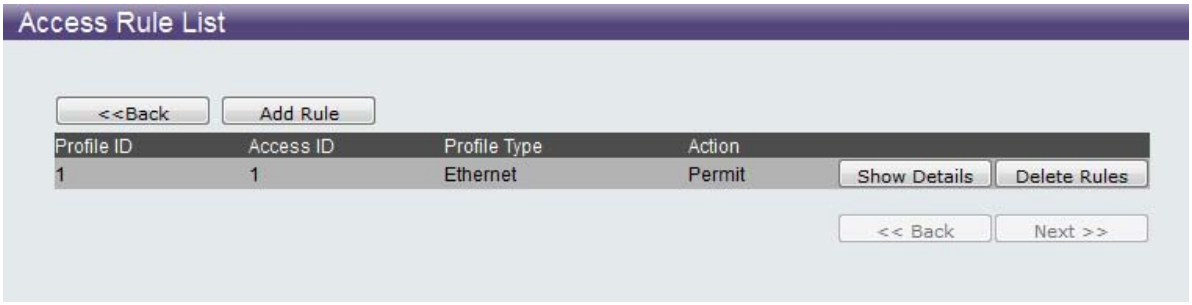


In this window, the following parameters can be configured:

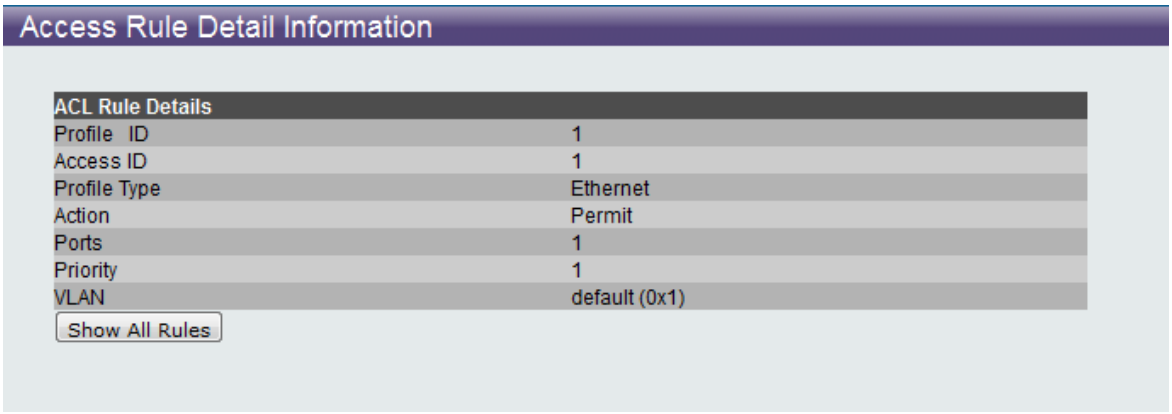
Parameters	Description
Access ID (1-65535)	Type in a unique identifier number for this access. This value can be set from *1* to *65535*. Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
VLAN Name	Selecting this option instructs the Switch to examine the VLAN part of each packet header and use this as the, or part of the, criterion for forwarding
VLAN ID (1-4094)	Mask ____ (0-FFF) – Specifies a VLAN ID.
VLAN ID	Allows the entry of a VLAN ID for a previously configured VLAN.
Source MAC Address	Specifies a MAC address mask for the source MAC address.
Source MAC Mask	Specifies a MAC address mask for the source MAC address. This mask is entered in a hexadecimal format.
Destination MAC Address	Specifies a MAC address for the destination MAC address.
Destination MAC Mask	Specifies a MAC address mask for the destination MAC address.
802.1p (0-7)	Enter a value from *0* to *7* to specify that the access profile will apply only to packets with this 802.1p priority value.
Ethernet Type (0-FFFF)	Enter a value that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value in the packet header.

Parameters	Description
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Priority (0-7)	Enter a priority value if you want to re-write the 802.1p user priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority	Click on the box to enable this option and manually enter the replacement value used to re-write the 802.1p user priority value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
Counter	Specifies whether counter feature will be enabled or disabled. This is optional, the default is disabled.
Ports	Enter a range of ports to be configured.

Click **Apply** to display the following **Access Rule List** window:

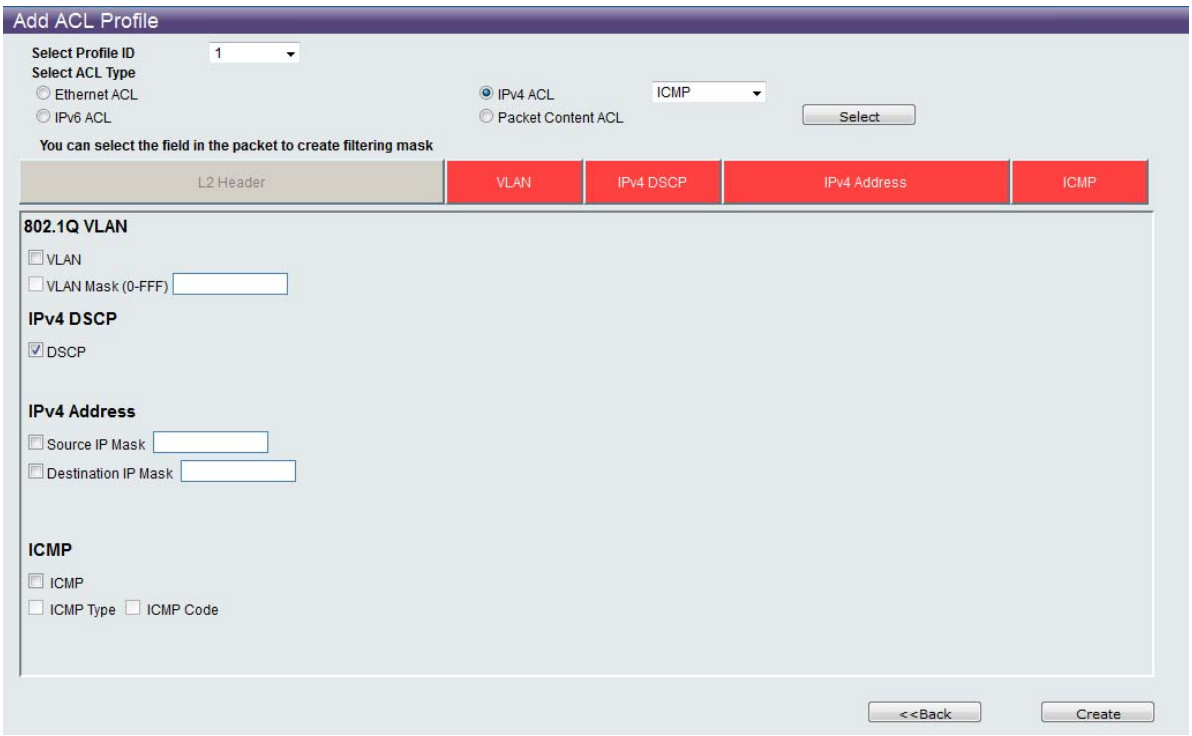


To view the configurations for previously configured rules, click on the corresponding **Show Details** button, which will display the following **Access Rule Detail Information** window:



Access Profile List – IPv4 ACL

To create an IPv4 ACL, click **Add ACL Profile** in the **Access Profile List** window and then use the drop-down menu to select a Profile ID between *1* and *256*, click the IPv4 ACL radio button, and then use the drop-down menu to select a protocol *ICMP*, *IGMP*, *TCP*, *UDP*, or *Protocol ID*. Click **Select** and the following window will appear (this window will vary depending on whether *ICMP*, *IGMP*, *TCP*, *UDP*, or *Protocol ID* has been selected):



Click on the boxes near the top of the window, which will then turn red and reveal parameters for configuration. To create a new entry, enter the appropriate information and click **Create**. To return to the **Access Profile List** window, click **<<Back**.

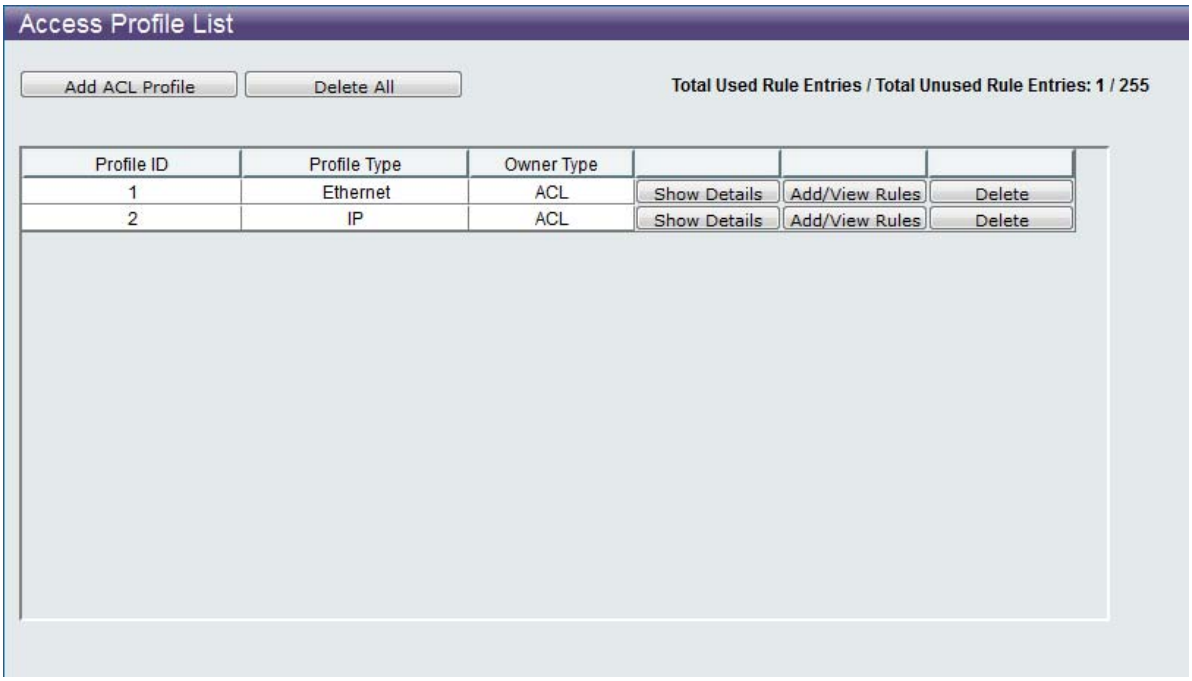
In this window, the following parameters can be configured:

Parameters	Description
VLAN	Selecting this option instructs the Switch to examine the VLAN part of each packet header and use this as the, or part of the, criterion for forwarding.
IPv4 DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
IPv4 Address	Tick either Source IP Mask and enter the IPv4 source address mask or Destination IP Mask and enter the IPV4 destination address mask.
ICMP	Tick ICMP to specify that the Switch will examine the Internet Control Message Protocol (ICMP) field within each packet.
	Tick ICMP Type to specify that the access profile will apply to this ICMP type value.
	Tick ICMP Code to specify that the access profile will apply to this ICMP code value.
IGMP	Tick IGMP to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header.
	Tick IGMP Type to further specify that the access profile will apply an IGMP type value.
TCP	Tick TCP to use the TCP port number contained in an incoming packet as the forwarding criterion. Ticking TCP requires specifying a source port mask and/ or a destination port mask. The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field.
	Source Port Mask (0-FFFF) - Tick and specify a TCP port mask for the source port to filter, in hex form (hex 0x0-0xffff).
	Destination Port Mask (0-FFFF) - Tick and specify a TCP port mask for the destination port to filter, in hex form (hex 0x0-0xffff).
	TCP Flag Bits – Tick URG (urgent), ACK (acknowledgement), PSH (push), RST (reset), SYN (synchronize), FIN (finish), or Check All to filter certain flag bits within the packets.
UDP	Tick UDP to use the UDP port number contained in an incoming packet as the forwarding criterion. Ticking UDP requires specifying a source port mask and/ or a destination port mask.
	Source Port Mask - Tick and specify a TCP port mask for the source port to filter, in hex form (hex 0x0-0xffff).
	Destination Port Mask - Tick and specify a TCP port mask for the destination port to filter, in hex form (hex 0x0-0xffff).
Protocol ID	Tick Protocol ID Mask and enter a value defining the protocol ID in the packet header to mask.
	Protocol ID Mask (0-FF) - Tick and enter a value defining the mask options behind the IP header.

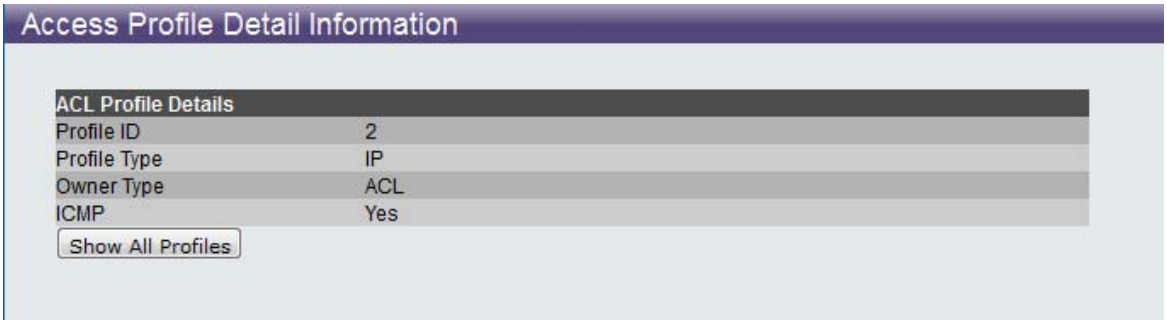
Click **Apply** to implement changes made.

Click **Create** to view the new Access Profile List entry in the **Access Profile List** window shown below. To add another Access Profile click **Add ACL Profile**. To delete a profile click the corresponding **Delete** button, to delete all the entries click on the **Delete All** button, to view the specific configurations for an entry click the **Show Details** button.

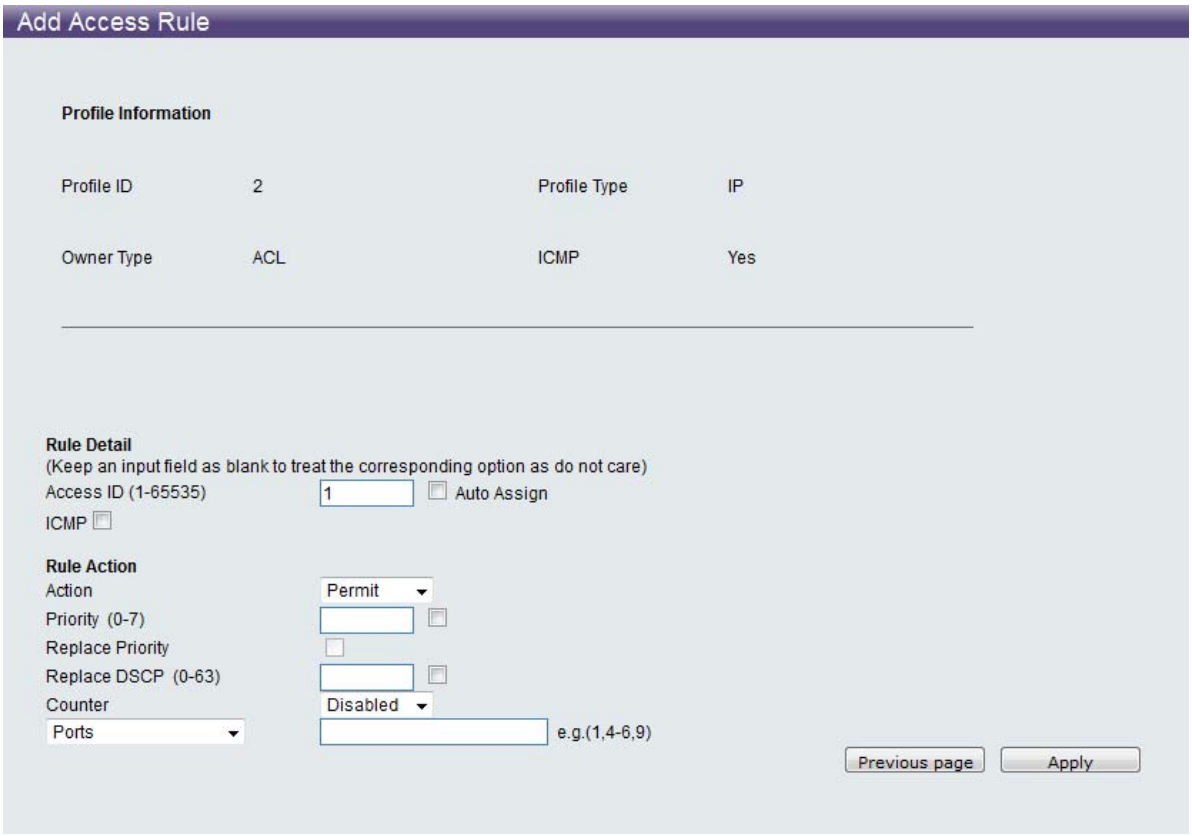
To add a rule to the Access Profile entry, click the **Add/View Rules** button.



To view the configurations for a previously configured entry, click on the corresponding **Show Details** button, which will display the following window:



To return to the **Access Profile List** window, click **Show All Profiles**. To add a rule to a previously configured entry, click on the corresponding **Add/View Rules** button, and then click **Add Rule** on the **Access Rule List** window, which will reveal the following window:



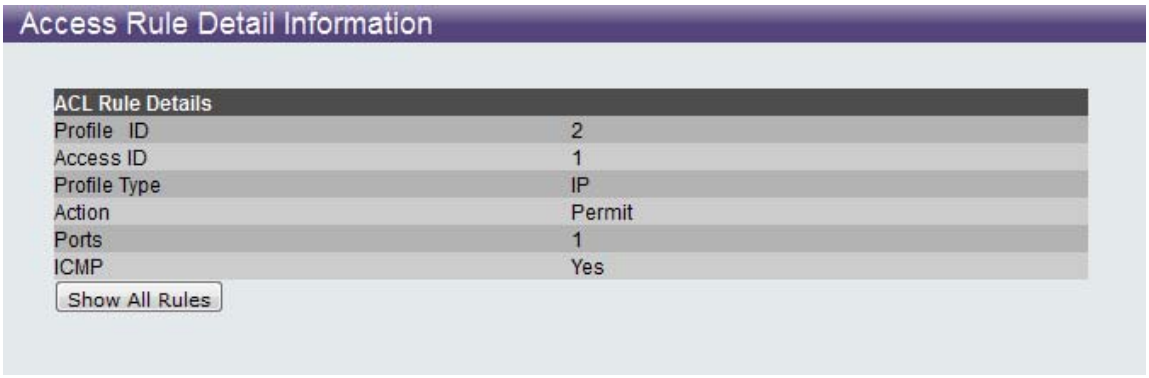
In this window, the following parameters can be configured:

Parameters	Description
Access ID (1-65535)	Type in a unique identifier number for this access. This value can be set from *1* to *65535*.
VLAN Name	Specifies a VLAN name.
VLAN ID (1-4094)	Mask ____ (0-FFF) – Specifies a VLAN ID.
Source IP Address	Specifies an IP address for the source IP address.
Source IP Mask	Specifies an IP address mask for the source IP address.
Destination IP Address	Specifies an IP address for the destination IP address.
Destination IP Mask	Specifies a destination IP address mask for the destination IP address.
DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the criteria, or part of the criterion for forwarding.
ICMP	Select *ICMP* to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header. ICMP Type - Specifies that the Switch will examine each frame's ICMP Type field. ICMP Code - Specifies that the Switch will examine each frame's ICMP Code field.

Parameters	Description
IGMP	Type ____ e.g. (0-255) - Specifies that the Switch will examine each frame's IGMP Type field.
TCP	Source Port - Specifies a TCP port for the source port.
	Mask (0-FFFF) - Specifies a TCP port mask for the source port.
	Destination Port - Specifies a TCP port for the destination port.
	Mask (0-FFFF) - Specifies a TCP port mask for the destination port.
	Flag Bits - Enter the appropriate flag mask parameter. All incoming packets have TCP port numbers contained in them as the forwarding criterion. These numbers have flag bits associated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets.
	URG/ACK/PSH/RST/SYN/FIN – Choose among *urg* (urgent), *ack* (acknowledgement), *psh* (push), *rst* (reset), *syn* (synchronize) and *fin* (finish)
UDP	Source Port - Specifies that the Switch will examine each frame's Universal Datagram Protocol (UDP) field for the source port.
	Mask (0-FFFF) - Specifies a UDP port mask for the destination port.
	Destination Port - Specifies a UDP port for the destination port.
	Mask (0-FFFF) - Specifies a UDP port mask for the destination port.
Protocol ID	Protocol ID ___ e.g. (0-255) - Specifies that the Switch will examine the protocol field in each packet and if this field contains the value entered here, apply the following rules.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below).
	Select *Deny* to specify the packets that match the access profile are not forwarded by the Switch and will be filtered.
	Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Priority (0-7)	Enter a priority value if you want to re-write the 802.1p user priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue.
Replace Priority	Click on the box to enable this option and manually enter the replacement value used to re-write the 802.1p user priority value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
Counter	Enable or disable the counter settings.
Ports	Enter a range of ports to be configured.

Click **Apply** to display the following **Access Rule List** window:

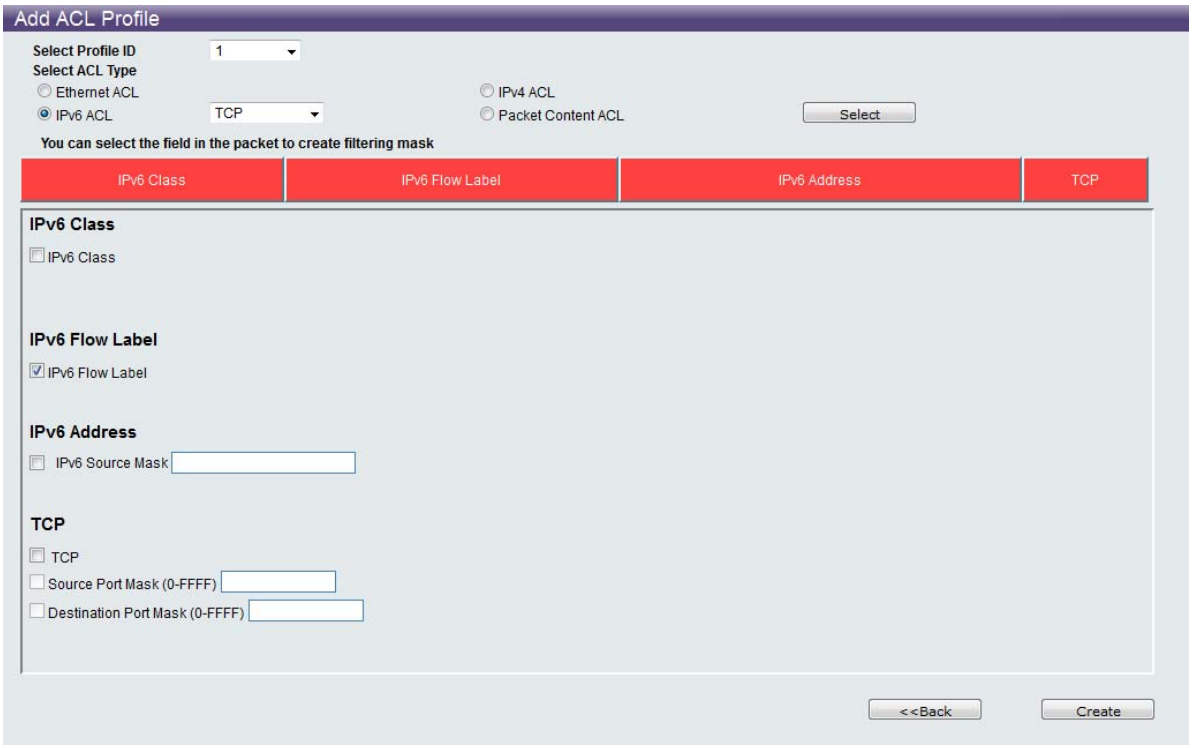
To view the configurations for a previously configured rule, click on the corresponding **Show Details** button, which will display the following **Access Rule Detail Information** window:



Access Profile List – IPv6 ACL

To create an IPv6 ACL, click **Add ACL Profile** in the **Access Profile List** window and then use the drop-down menu to select a Profile ID between *1* and *256*, click the IPv6 ACL radio button, and then use the drop-down menu to select a protocol *TCP* or *UDP*.

Click **Select** and the following window will appear (this window will vary depending on whether *TCP* or *UDP* has been selected):



Click on the boxes at the top of the table, which will then turn red and reveal parameters for configuration. To create a new entry enter the correct information and click **Create**. To return to the **Access Profile List** window, click **<<Back**.

In this window, the following parameters can be configured:

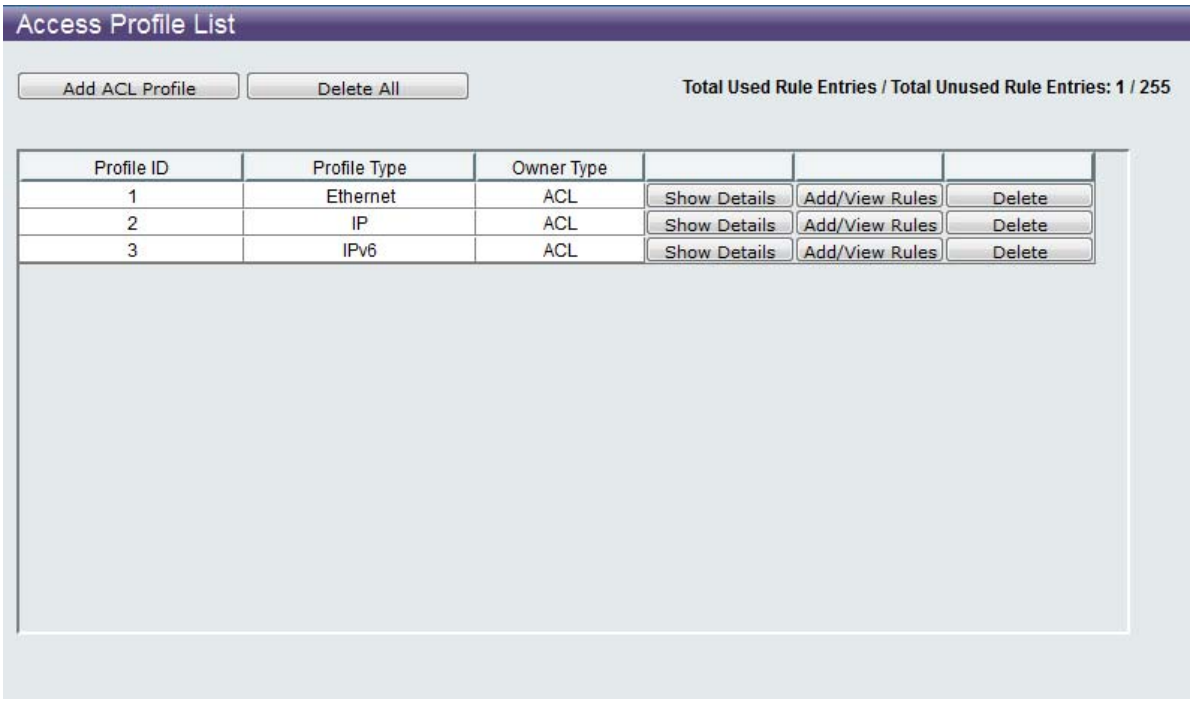
Parameters	Description
IPv6 Class	Ticking this check box will instruct the Switch to examine the class field of the IPv6 header. The class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
IPv6 Flow Label	Ticking this check box will instruct the Switch to examine the flow label field of the IPv6 header. The flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
IPv6 Address	Ticking this check box will instruct the Switch to examine the IPv6 Source Address.
IPv6 TCP	Ticking this check box will specify that the rule applies to TCP traffic. The user can tick and enter a specific TCP Source Port Mask or TCP Destination Port Mask.
IPv6 UDP	Ticking this check box will specify that the rule applies to UDP traffic. The user can tick and enter a specific UDP Source Port Mask or UDP Destination Port Mask.

Click **Apply** to implement changes made.

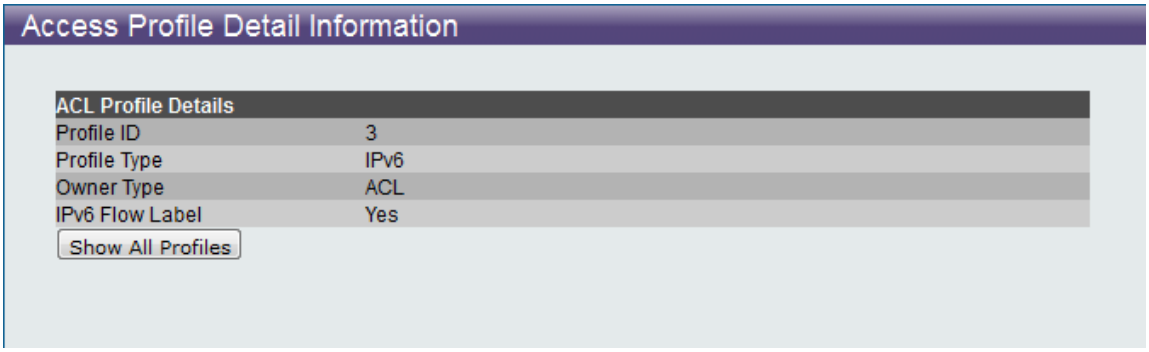
Click **Create** to view the new Access Profile List entry in the **Access Profile List** window shown below. To add another Access Profile, click **Add ACL Profile**. To delete a profile click the corresponding **Delete**

button. To delete all the entries click on the **Delete All** button. To view the specific configurations for an entry click, the **Show Details** button.

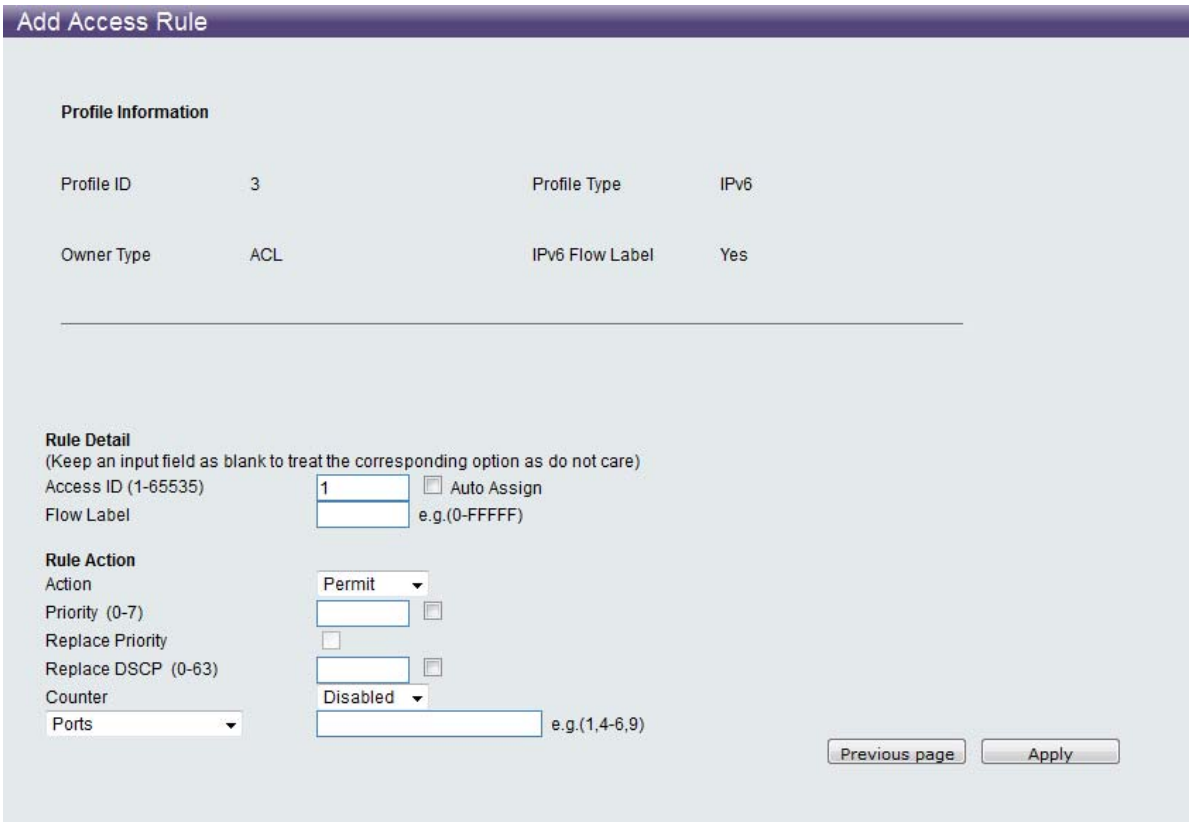
To add a rule to the Access Profile entry, click the **Add/View Rules** button.



To view the configurations for a previously configured entry, click on the corresponding **Show Details** button, which will display the following window:



To return to the **Access Profile List** window, click **Show All Profiles**. To add a rule to a previously configured entry, click on the corresponding **Add/View Rules** button and then click **Add Rule** on the **Access Rule List** window, which will reveal the following window:



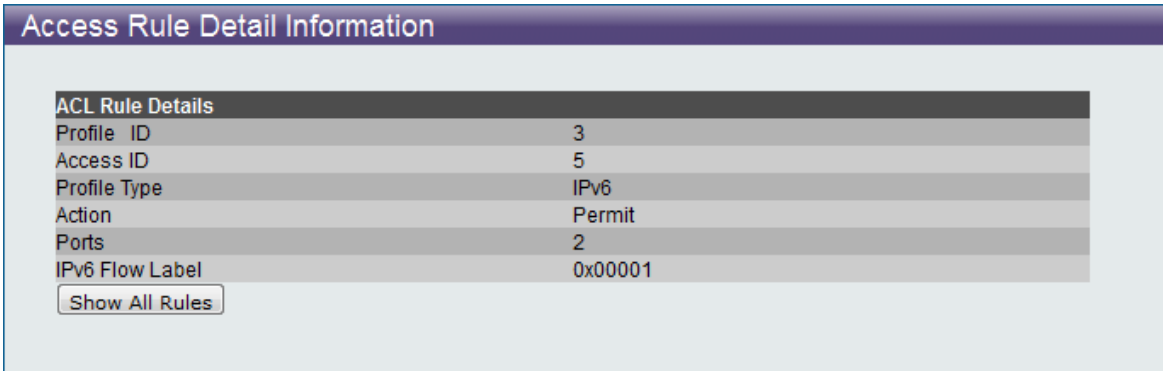
In this window, the following parameters can be configured:

Parameters	Description
Access ID (1-65535)	Type in a unique identifier number for this access. This value can be set from *1* to *65535*.
	Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Class	Entering a class will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
Flow Label	Specifies the IPv6 Flow Label. Enter a value between *0* – *FFFFF*.
IPv6 Source Address	Specifies an IPv6 address for the IPv6 source address.
IPv6 Source Mask	Specifies an IPv6 source submask.
TCP	Source Port - Specifies an IPv6 L4 TCP source port submask.
	Destination Port - Specifies an IPv6 L4 TCP destination port submask.
UDP	Source Port - Specifies an IPv6 L4 UDP source port submask.
	Destination Port - Specifies an IPv6 L4 UDP destination port submask.

Parameters	Description
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Priority (0-7)	Enter a priority value if you want to re-write the 802.1p user priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue.
Replace Priority	Click on the box to enable this option and manually enter the replacement value used to re-write the 802.1p user priority value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
Counter	Enable or disable the counter settings.
Ports	Enter a range of ports to be configured.

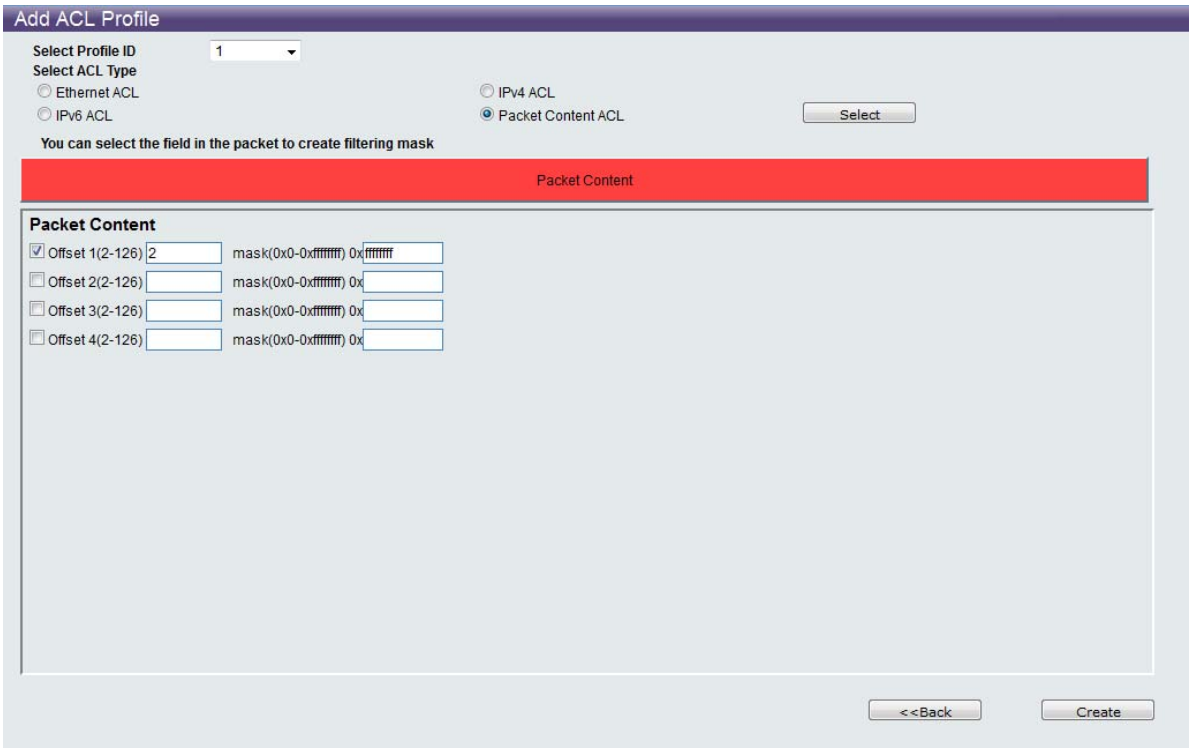
Click **Apply** to display the following **Access Rule List** window:

To view the configurations for a previously configured rule, click on the corresponding **Show Details** button, which will display the following **Access Rule Detail Information** window:



Access Profile List – Packet Content ACL

To create a Packet Content ACL, click **Add ACL Profile** in the **Access Profile List** window and then use the drop-down menu to select a Profile ID between *1* and *256* and click the Packet Content ACL radio button. Click **Select** and the following window will appear:



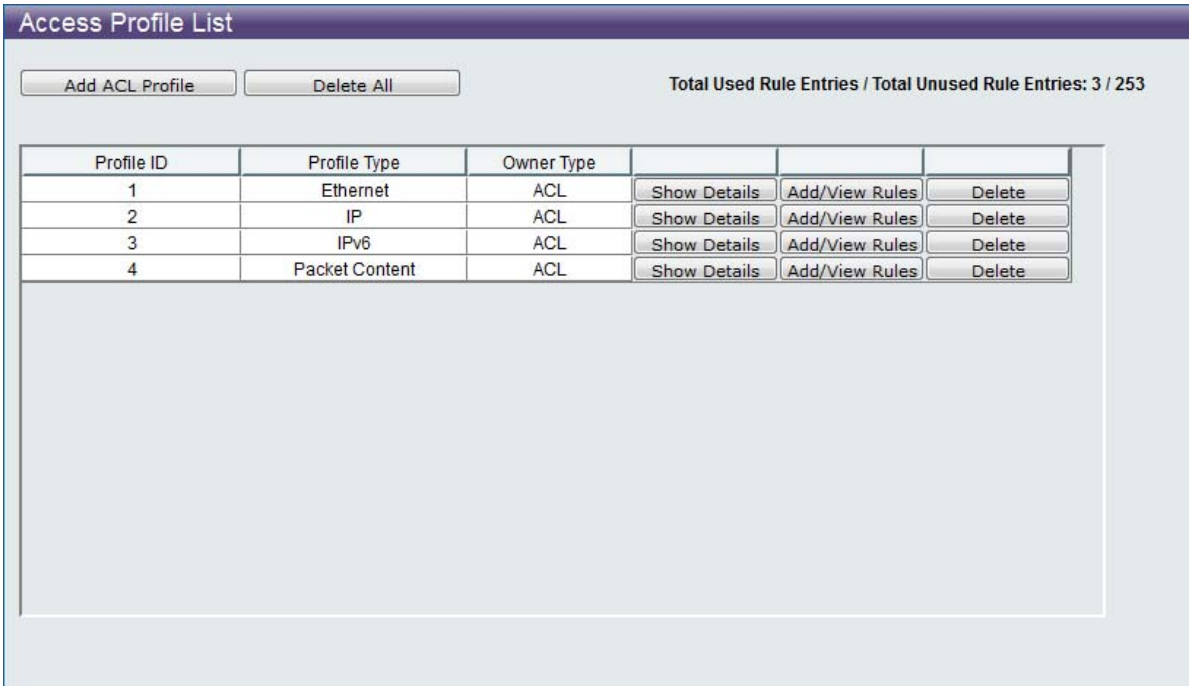
Click on the boxes at the top of the table, which will then turn red and reveal parameters for configuration. To create a new entry enter the correct information and click **Create**. To return to the **Access Profile List** window, click **<<Back**.

In this window, the following parameters can be configured:

Parameters	Description
Packet Content	Allows users to examine up to four specified offset packet content chunks within a packet at one time and specifies the offset and mask. The four offsets can be selected in the following format: Offset 1 (2-126) _____mask_____ Offset 2 (2-126) _____mask_____ Offset 3 (2-126) _____mask_____ Offset 4 (2-126) _____mask_____ With this advanced unique Packet Content Mask (also known as Packet Content Access Control List - ACL), the Switch can effectively mitigate some network attacks like the common ARP Spoofing attack that is wide spread today. This is why the Packet Content ACL is able to inspect any specified content of a packet in different protocol layers.

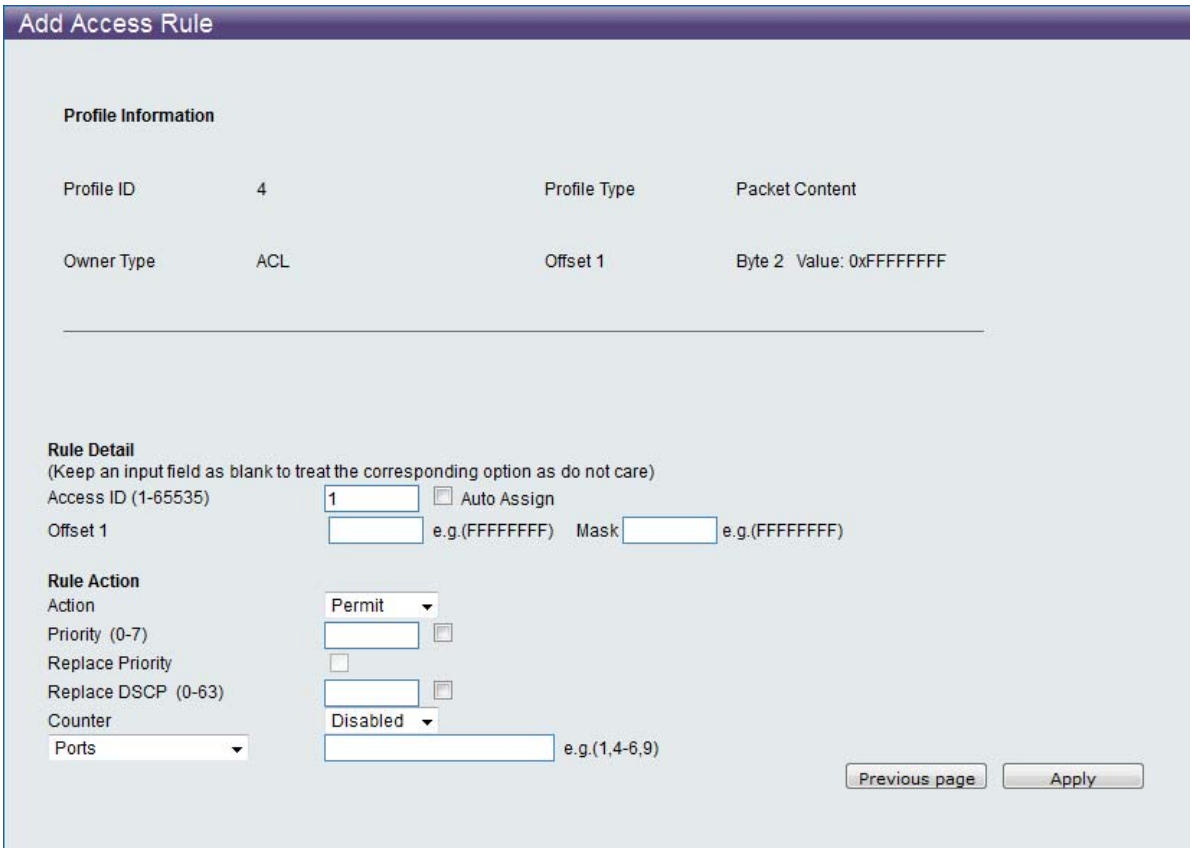
Click **Apply** to implement changes made.

Click **Create** to view the new Access Profile List entry in the **Access Profile List** window shown below. To add another Access Profile, click **Add ACL Profile**. To delete a profile, click the corresponding **Delete** button. To delete all the entries click on the **Delete All** button. To view the specific configurations for an entry, click the **Show Details** button. To add a rule to the Access Profile entry, click the **Add/View Rules** button.



To view the configurations for a previously configured entry, click on the corresponding **Show Details** button, which will display the following window:

To return to the **Access Profile List** window, click **Show All Profiles**. To add a rule to a previously configured entry, click on the corresponding **Add/View Rules** button and then **Add Rule**, which will reveal the following window:



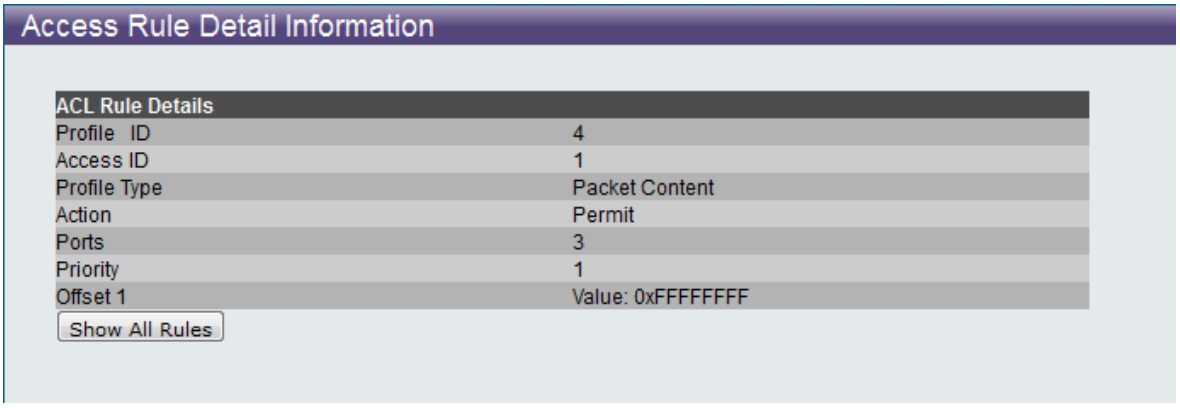
In this window, the following parameters can be configured:

Parameters	Description
Access ID (1-65535)	Type in a unique identifier number for this access. This value can be set from *1* to *65535*.
Offset (1–4)	Each UDF field is a 4-byte data which is n bytes away from the offset reference (where n is the offset value). A total of 4 packet content fields can be selected from the first 128 bytes of a packet. The first offset starts at 2. The packet content fields should have no overlaps, and since each field is 4 bytes, the valid offset values are: 2,6,10,14,18,22,26,30,34…,126
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Priority (0-7)	Enter a priority value if you want to re-write the 802.1p user priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue.

Parameters	Description
Replace DSCP	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
Counter	Enable or disable the counter for this ACL rule.
Ports	Enter a range of ports to be configured.

Click **Apply** to display the following **Access Rule List** window:

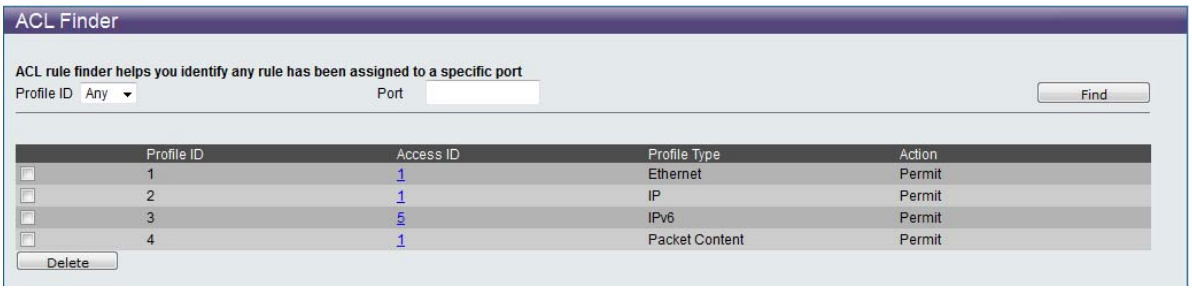
To view the configurations for a previously configured rule, click on the corresponding **Show Details** button, which will display the following **Access Rule Detail Information** window:



ACL Finder

This window is used to help find a previously configured ACL entry.

To open this window, click **ACL > ACL Finder**

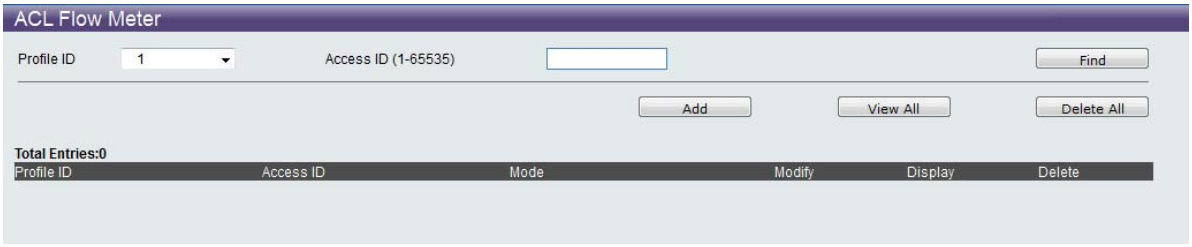


To search for an entry, select the profile ID from the drop-down menu, enter a port to view, and click **Find,** the table on the lower half of the window will display the entries. To delete an entry click the corresponding **Delete** button.

ACL Flow Meter

This window offers flow bandwidth control used to limit the bandwidth of the ingress traffic. When users create an ACL rule to filter packets, a metering rule can be created to associate with this ACL rule to limit traffic. Due to limited metering rules, not all ACL rules can associate with a metering rule.

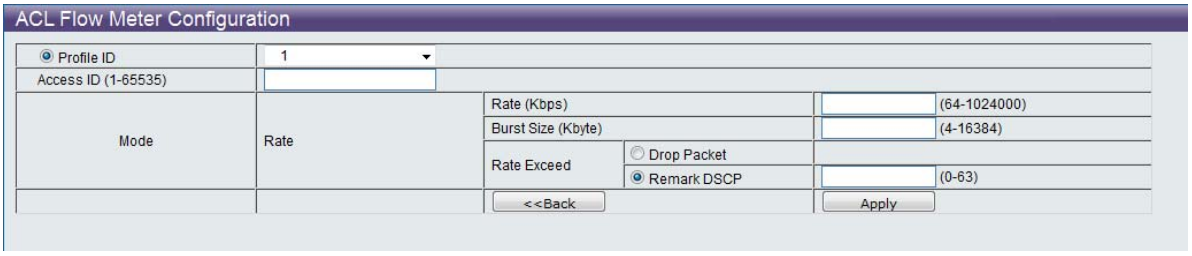
To open this window, click **ACL > ACL Flow Meter**



In this window, the following parameters can be configured:

Parameters	Description
Profile ID	The pre-configured Profile ID for which to configure the Flow Metering parameters.
Access ID (1-65535)	The pre-configured Access ID for which to configure the Flow Metering parameters.

Enter the appropriate information and click **Find**. The entries will be displayed on the lower half of the table. To edit an entry, click the corresponding **Modify** button. To delete an entry, click the corresponding **Delete** button. To add a new entry, click the **Add** button, which will display the following window for the user to configure:



In this window, the following parameters can be configured:

Parameters		Description
Profile ID		Use the drop-down menu to select the pre-configured Profile ID that will be used to configure the Flow Metering parameters.
Access ID	**(1-65535)**	Enter the Access ID that will be used to configure the Flow Metering parameters, enter a value between *1* and *65535*.

Parameters	Description
Mode	*Rate (Kbps)* – Specifies the committed bandwidth in Kbps for the flow. The range is from *64* to *1024000*. The unit is Kbps.
	Burst Size (Kbyte) – Specifies the burst size for this flow. The range is from *4* to *16384*. The unit is Kbyte.
Rate Exceed:	*Drop Packet*– Drops the packet.
	Remark DSCP – Change the DSCP of the packet.

Click **Apply** to implement changes made, click **<<Back** to return to the **ACL Flow Meter** window.

7 Monitoring

CHAPTER

Cable Diagnostics

This window displays the details of copper cables attached to specific ports on the Switch. If there is an error in the cable this feature can determine the type of error and the position where the error has occurred.

To view this window, click **Monitoring > Cable Diagnostics**:

Cable Diagnostics
From Port
01
To Port
01
Test
Port
Type
Link Status
Test Result
Cable Length(M)
The Cable Diagnostics is designed primarily for administrators or customer service representative to view tests on copper cables, it can rapidly determine where errors occurred in the cable and the type of cable error which occurred.
Note:
The Cable Fault Distance is calculated from switch side.

Enter the range of ports to test and click **Test**. The results will be displayed in the table on the lower half of the window.

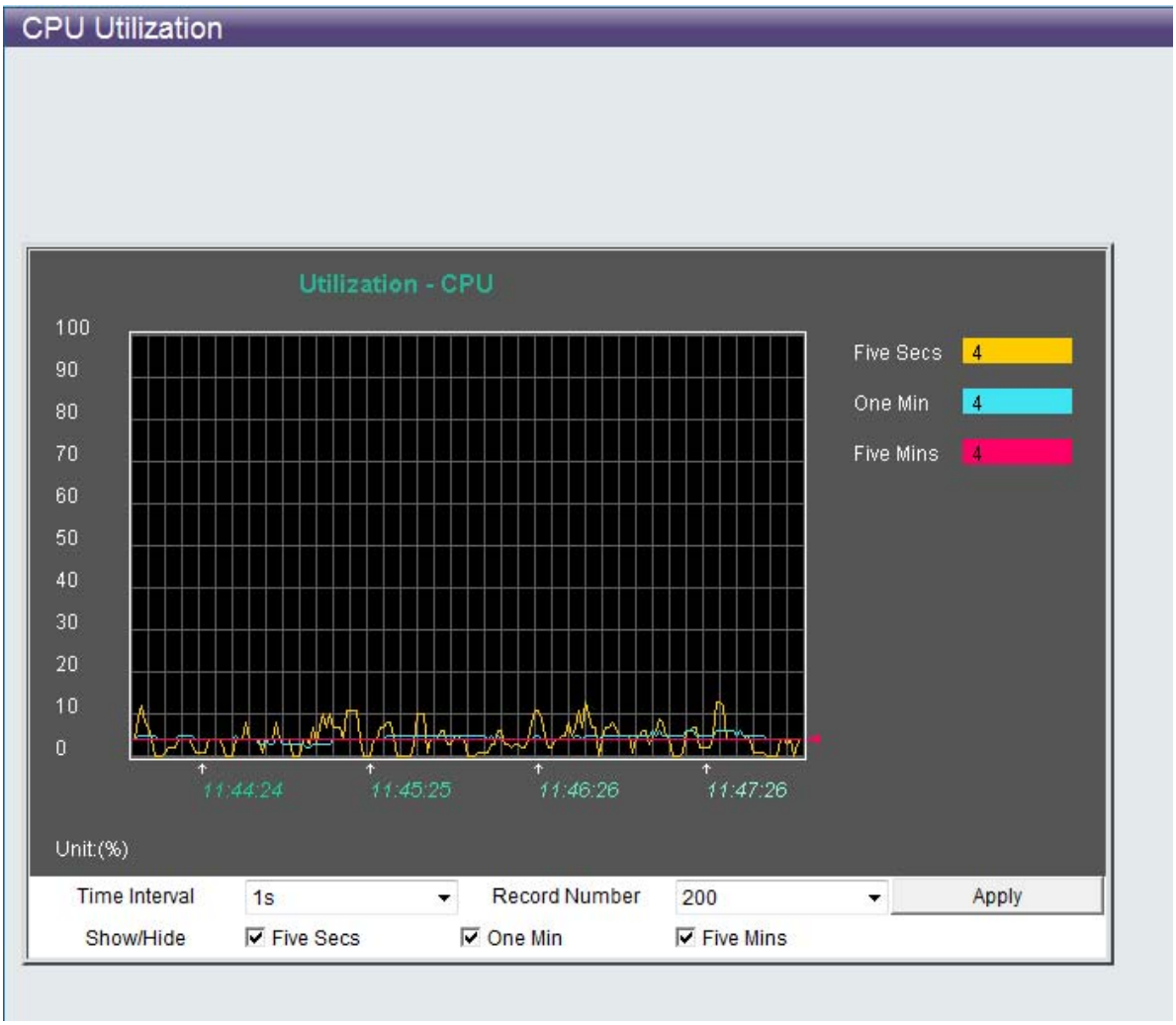
NOTE

If the Link Status field for an interface displays "**Link Up**", the value displayed in the Cable Length field may not be accurate for the interface

CPU Utilization

This window displays the percentage of the CPU being used, expressed as an integer percentage and calculated as a simple average by time interval.

To view this window, click **Monitoring > CPU Utilization**:



To view the CPU utilization by port, use the real-time graphic of the Switch at the top of the Web page by simply clicking on a port. The window will automatically refresh with new updated statistics.

In this window, the following parameters can be configured:

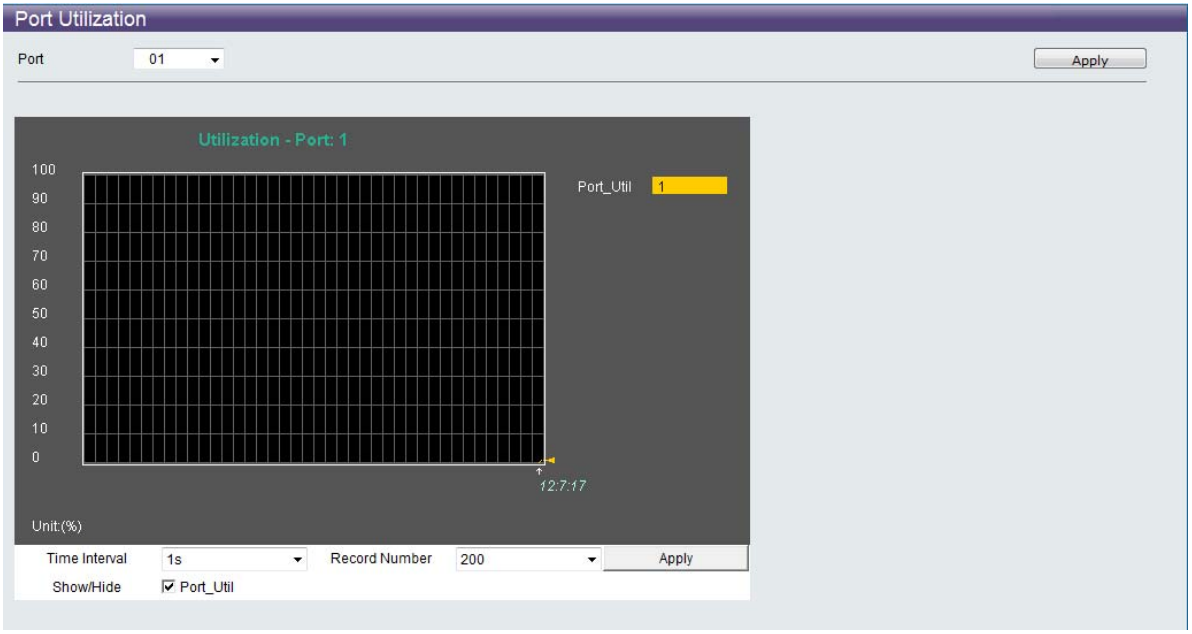
Parameters	Description
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Check whether or not to display Five Secs, One Min, and Five Mins.

Click on the **Apply** button to accept the changes made.

Port Utilization

This window displays the percentage of the total available bandwidth being used on the port.

To view this window, click **Monitoring > Port Utilization**:



To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the Web page by simply clicking on a port.

In this window, the following parameters can be configured:

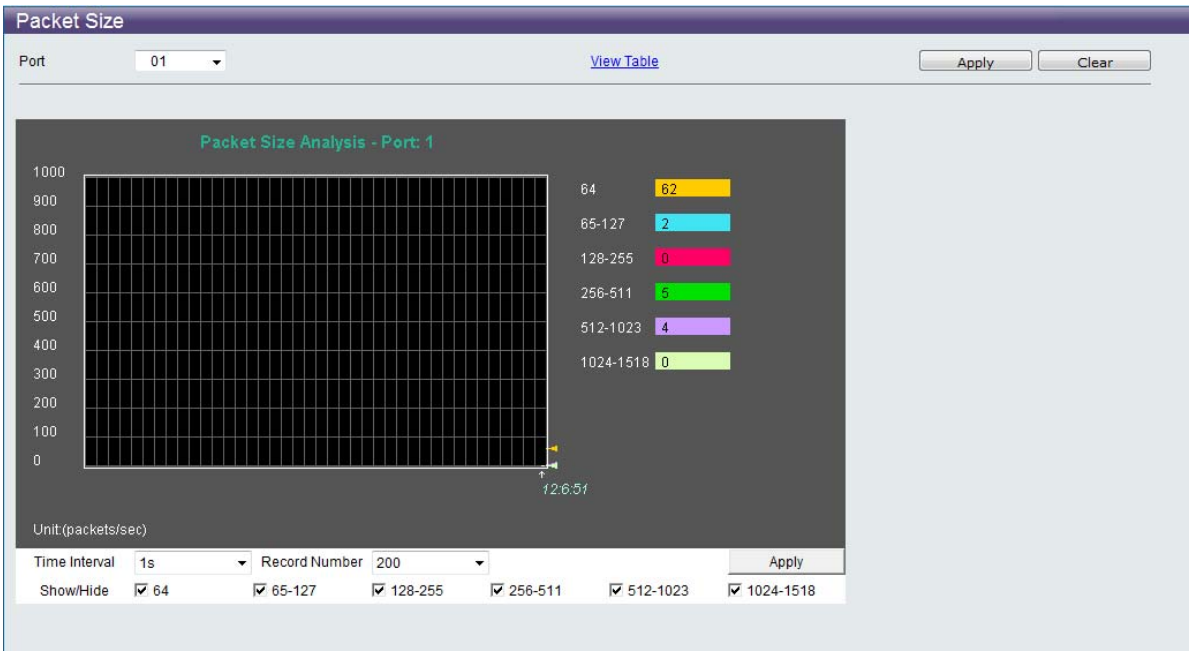
Parameters	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Check whether or not to display Utilization.

Click on the **Apply** button to accept the changes made.

Packet Size

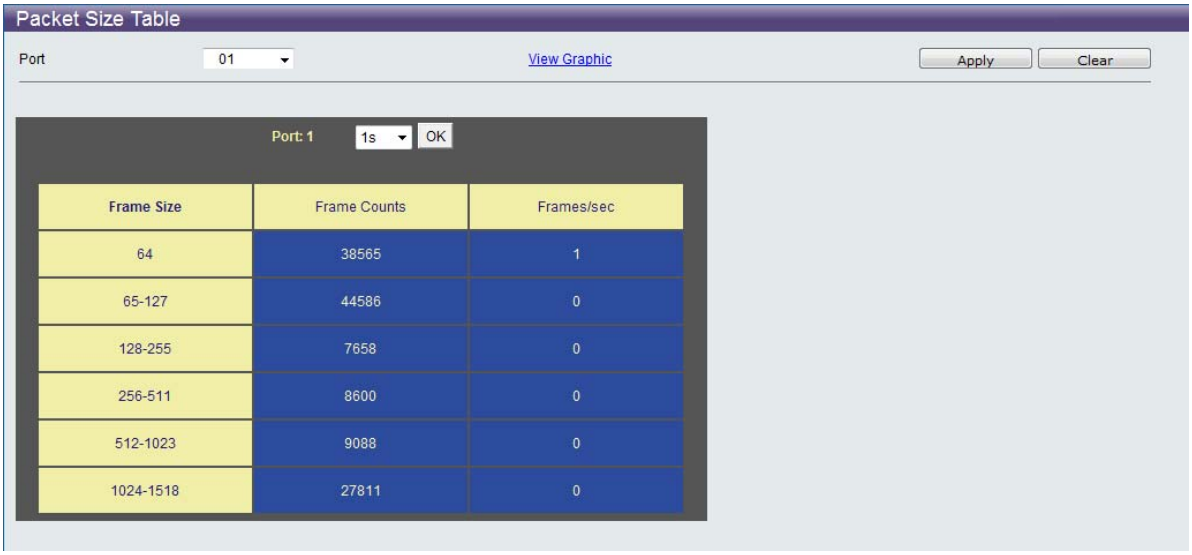
The Web Manager allows packets received by the Switch, arranged in six groups and classed by size, to be viewed as either a line graph or a table. Two windows are offered. To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the Web page by simply clicking on a port.

To view the packet size windows, click **Monitoring > Packet Size**:



Click on the **Apply** button to accept the changes made.

To view the **Packet Size Table** window, click the link View Table, which will show the following table:



In this window, the following parameters can be configured:

Parameters	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is 200.

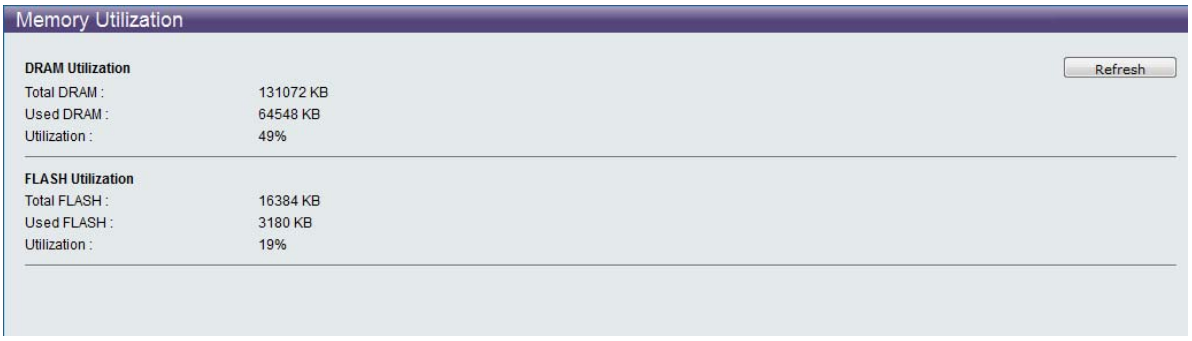
Parameters	Description
64	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
65-127	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Show/Hide	Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the Switch to display a line graph rather than a table.

Click on the **Apply** button to accept the changes made.

Memory Utilization

The Switch displays memory utilization information for DRAM and Flash.

To view this window, click **Monitoring > Memory Utilization**:



Click on the **Refresh** button to refresh the display list.

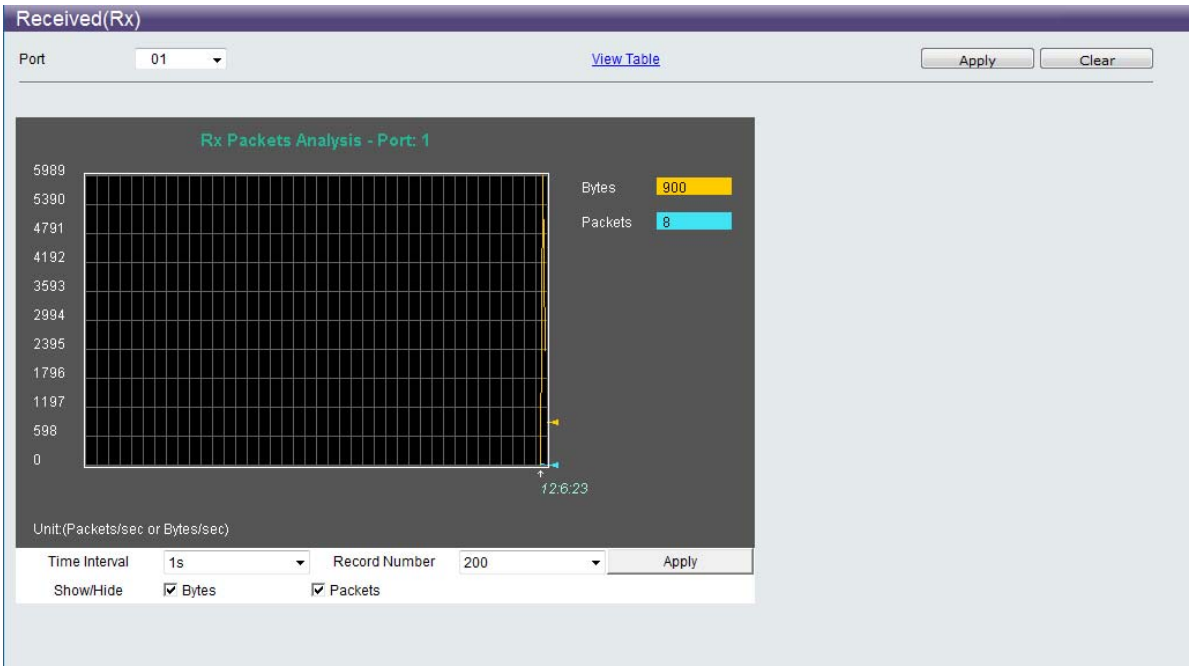
Packets Folder

The Web Manager allows various packet statistics to be viewed as either a line graph or a table. Six windows are offered.

Received (Rx)

These windows display the Rx packets on the Switch. To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the Web page by simply clicking on a port.

To view the following graph of packets received on the Switch, click **Monitoring > Packets > Received (Rx)**:



Click on the **Apply** button to accept the changes made.

Click on the **Clear** button to clear the data.

To view the **Received (Rx) Table** window, click View Table.

In this window, the following parameters can be configured:

Parameters	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "*s*" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Bytes	Counts the number of bytes received on the port.
Packets	Counts the number of packets received on the port.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether to display Bytes and Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the Switch to display a line graph rather than a table.

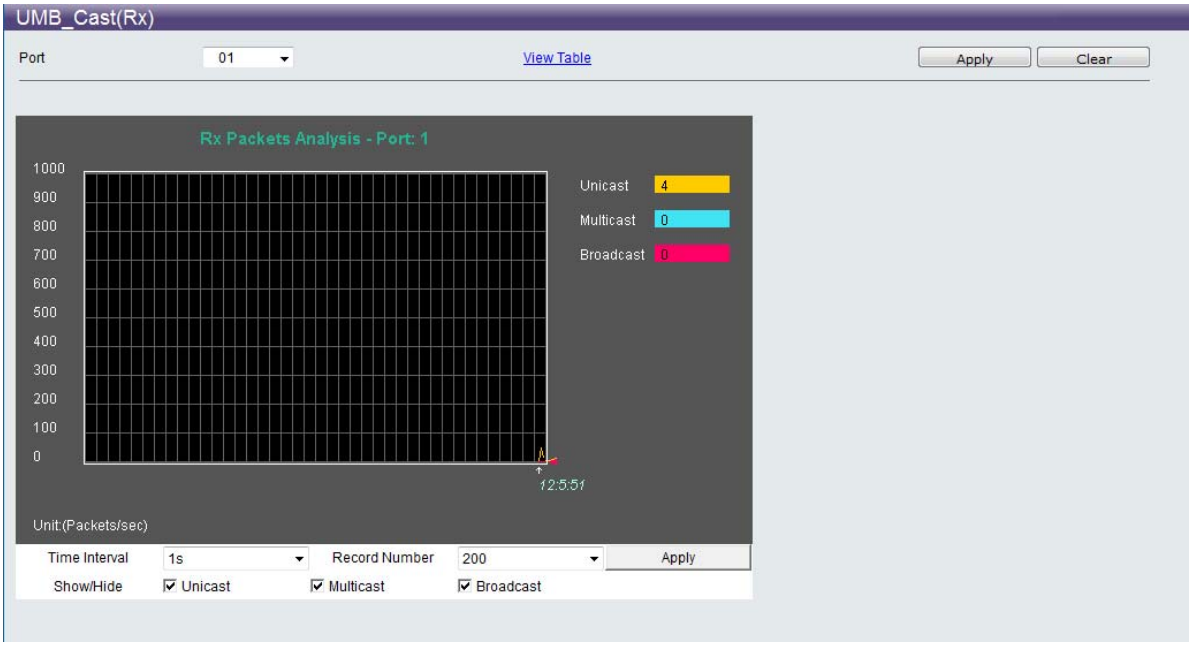
Click on the **Apply** button to accept the changes made.

Click on the **Clear** button to clear the data.

UMB_cast (Rx)

These windows display the UMB_cast Rx packets on the Switch. To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the Web page by simply clicking on a port.

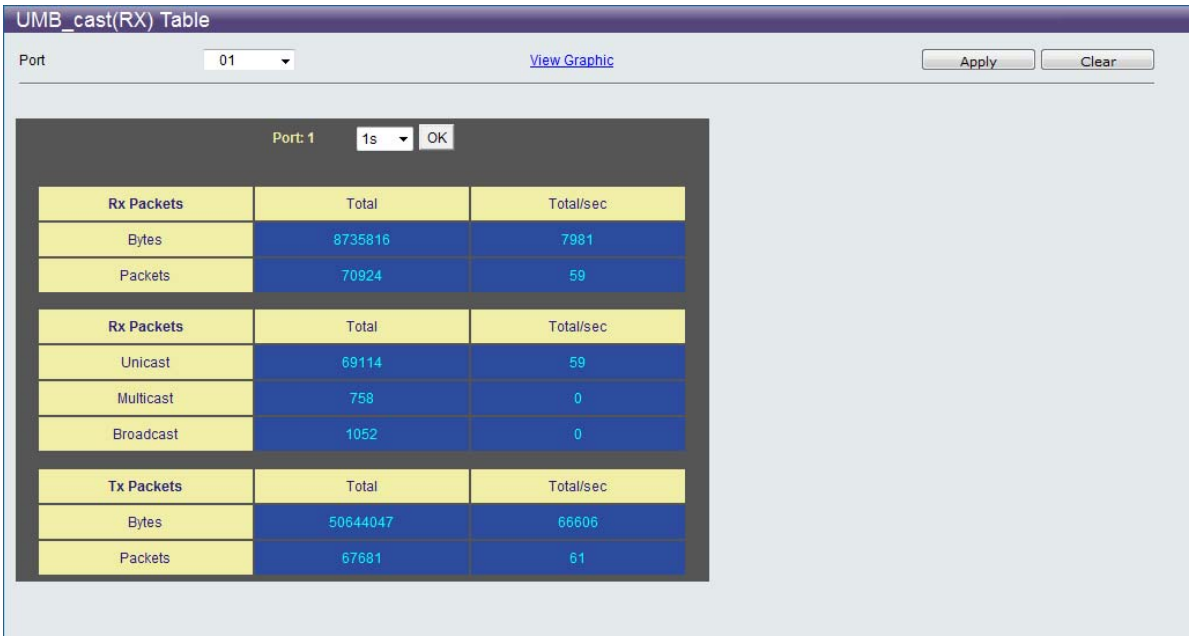
To view the following graph of UMB cast packets received on the Switch, click **Monitoring > Packets > UMB_cast (Rx)**:



Click on the **Apply** button to accept the changes made.

Click on the **Clear** button to clear the data.

To view the **UMB_cast (Rx) Table** window, click the View Table link.



In this window, the following parameters can be configured:

Parameters	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "*s*" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether or not to display Multicast, Broadcast, and Unicast Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the Switch to display a line graph rather than a table.

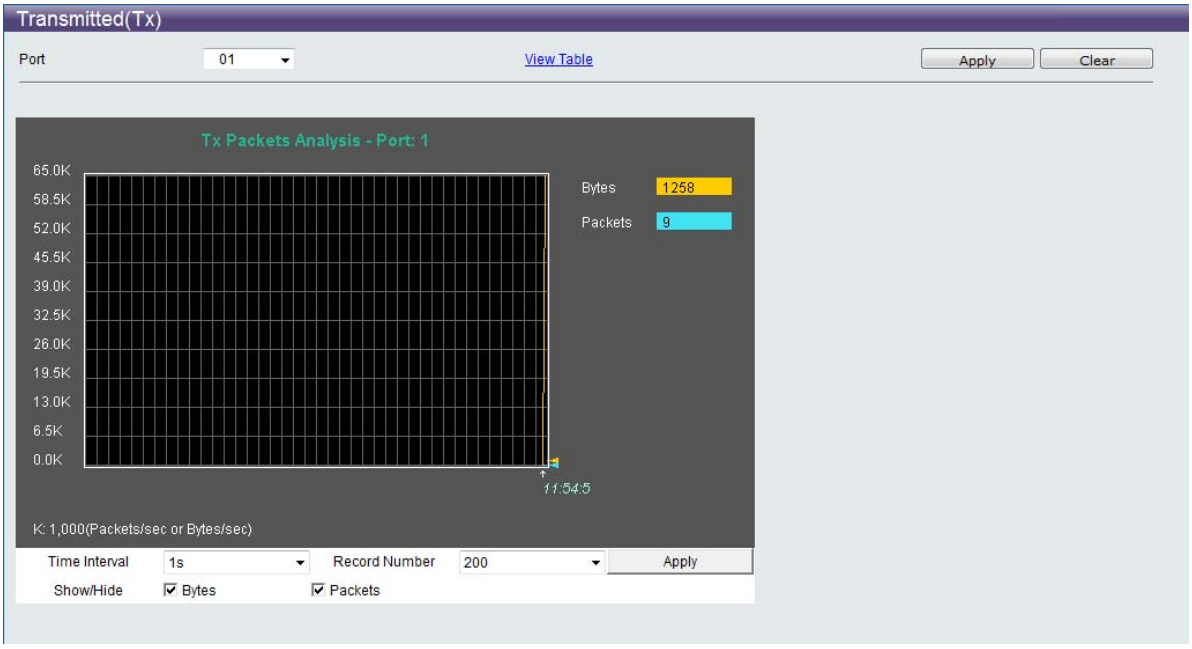
Click on the **Apply** button to accept the changes made.

Click on the **Clear** button to clear the data.

Transmitted (Tx)

These windows display the Transmittd (Tx) packets on the Switch.To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the Web page by simply clicking on a port.

To view the following graph of packets transmitted from the Switch, click **Monitoring > Packets > Transmitted (Tx)**:



Click on the **Apply** button to accept the changes made.

Click on the **Clear** button to clear the data.

To view the **Transmitted (Tx) Table** window, click the link View Table.

In this window, the following parameters can be configured:

Parameters	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "*s*" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Bytes	Counts the number of bytes successfully sent on the port.
Packets	Counts the number of packets successfully sent on the port.
Unicast	Counts the total number of good packets that were transmitted by a unicast address.
Multicast	Counts the total number of good packets that were transmitted by a multicast address.
Broadcast	Counts the total number of good packets that were transmitted by a broadcast address.
Show/Hide	Check whether or not to display Bytes and Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the Switch to display a line graph rather than a table.

Click on the **Apply** button to accept the changes made.

Click on the **Clear** button to clear the data.

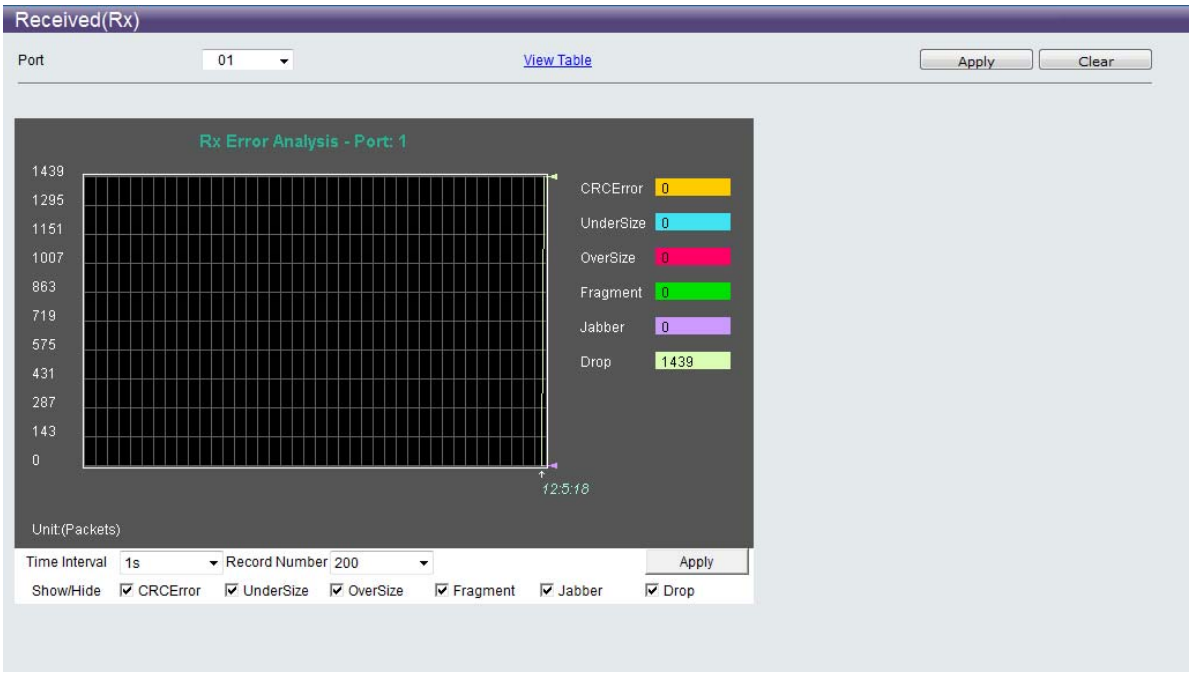
Errors Folder

The Web Manager allows port error statistics compiled by the Switch's management agent to be viewed as either a line graph or a table. Four windows are offered.

Received (RX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the Web page by simply clicking on a port.

To view the following graph of error packets received on the Switch, click **Monitoring > Errors > Received (RX)**:



Click on the **Apply** button to accept the changes made.

Click on the **Clear** button to clear the data.

To view the **Received (Rx) Table** window for errors, click the link View Table, which will show the following table:

In this window, the following parameters can be configured:

Parameters	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "*s*" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
CRCError	Counts otherwise valid packets that did not end on a byte (octet) boundary.
UnderSize	The number of packets detected that are less than the minimum permitted packets size of 64 bytes and have a good CRC. Undersize packets usually indicate collision fragments, a normal network occurrence.
OverSize	Counts valid packets received that were longer than 1518 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1536.
Fragment	The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
Jabber	Counts invalid packets received that were longer than 1518 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1536.
Drop	The number of packets that are dropped by this port since the last Switch reboot.
Show/Hide	Check whether or not to display CRCError, UnderSize, OverSize, Fragment, Jabber, Drop, and SymbolErr errors.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the Switch to display a line graph rather than a table.

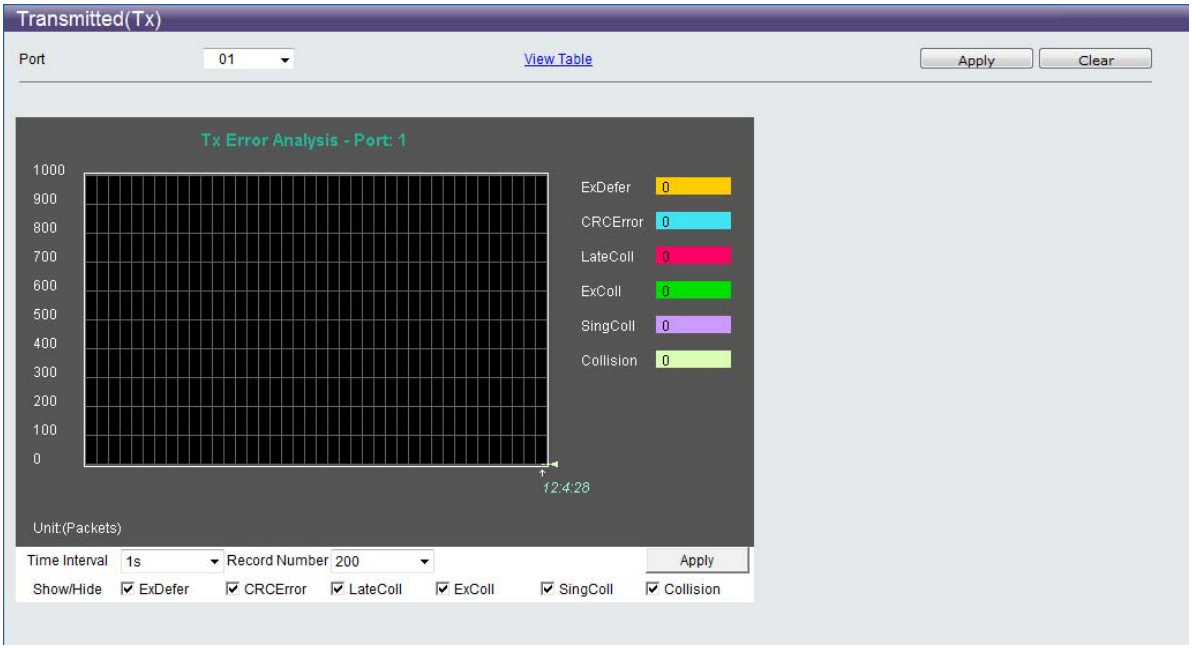
Click on the **Apply** button to accept the changes made.

Click on the **Clear** button to clear the data.

Transmitted (TX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the Web page by simply clicking on a port.

To view the following graph of error packets received on the Switch, click the **Monitoring > Errors > Transmitted (Tx)** :



Click on the **Apply** button to accept the changes made.

Click on the **Clear** button to clear the data.

To view the **Transmitted (Tx) Table** window, click the link View Table, which will show the following table:

In this window, the following parameters can be configured:

Parameters	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
ExDefer	Counts the number of packets for which the first transmission attempt on a particular interface was delayed because the medium was busy.
CRC Error	Counts otherwise valid packets that did not end on a byte (octet) boundary.
LateColl	Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
ExColl	Excessive Collisions. The number of packets for which transmission failed due to excessive collisions.
SingColl	Single Collision Frames. The number of successfully transmitted packets for which transmission is inhibited by more than one collision.
Collision	An estimate of the total number of collisions on this network segment.
Show/Hide	Check whether or not to display ExDefer, CRCError, LateColl, ExColl, SingColl, and Collision errors.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the Switch to display a line graph rather than a table.

Click on the **Apply** button to accept the changes made.

Click on the **Clear** button to clear the data.

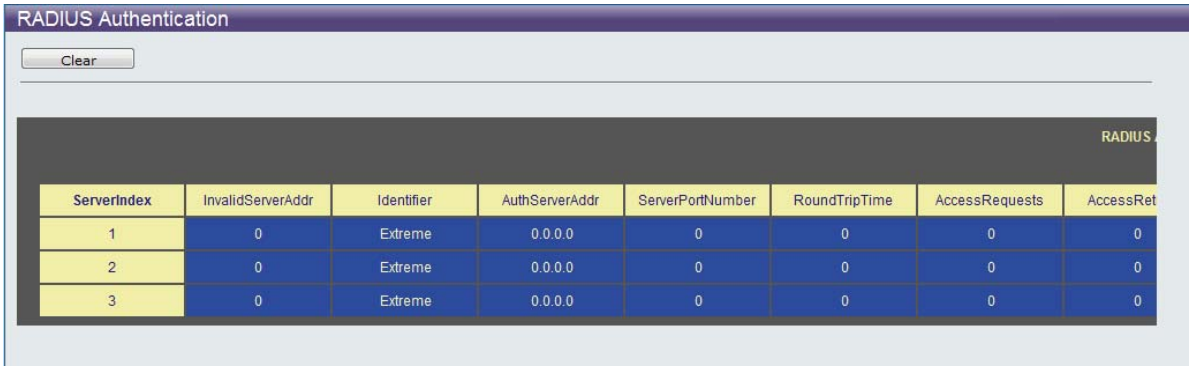
Port Access Control Folder

The following six windows are used to monitor 802.1X statistics of the Switch, on a per port basis.

RADIUS Authentication

This table contains information concerning the activity of the RADIUS authentication client on the client side of the RADIUS authentication protocol.

To view the **RADIUS Authentication** window, click **Monitoring > Port Access Control > RADIUS Authentication**:



The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second. To clear the current statistics shown, click the **Clear** button in the top left hand corner.

In this window, the following parameters can be configured:

Parameters	Description
InvalidServerAddresses	The number of RADIUS Access-Response packets received from unknown addresses.
Identifier	The NAS-Identifier of the RADIUS authentication client. (This is not necessarily the same as sysName in MIB II.)
ServerIndex	The identification number assigned to each RADIUS Authentication server that the client shares a secret with.
AuthServerAddress	The (conceptual) table listing the RADIUS authentication servers with which the client shares a secret.
ServerPortNumber	The UDP port the client is using to send requests to this server.
RoundTripTime	The time interval (in hundredths of a second) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
AccessRequests	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
AccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
AccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
AccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.

Parameters	Description
AccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
AccessResponses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or known types are not included as malformed access responses.
BadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.
PendingRequests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject or Access-Challenge, a timeout or retransmission.
Timeouts	The number of authentication timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
UnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the authentication port
PacketsDropped	The number of RADIUS packets of which were received from this server on the authentication port and dropped for some other reason.

RADIUS Account Client

This window shows managed objects used for managing RADIUS accounting clients, and the current statistics associated with them.

To view the **RADIUS Account Client** window, click **Monitoring > Port Access Control > RADIUS Account Client**:

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second. To clear the current statistics shown, click the **Clear** button in the top left hand corner.

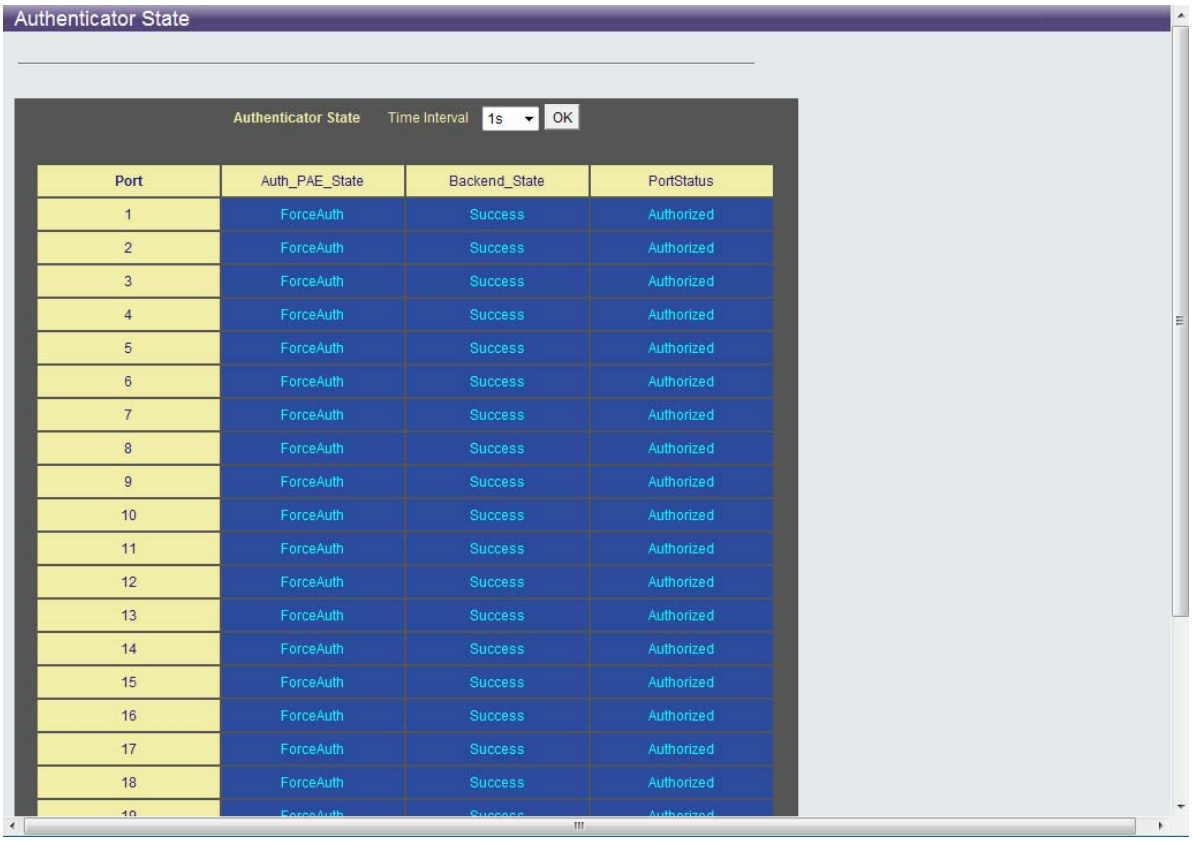
In this window, the following parameters can be configured:

Parameters	Description
InvalidServerAddresses	The number of RADIUS Accounting-Response packets received from unknown addresses.
Identifier	The NAS-Identifier of the RADIUS account. (This is not necessarily the same as sysName in MIB II.)
ServerIndex	The identification number assigned to each RADIUS Accounting server that it shares a secret with.
ServerAddress	The (conceptual) table listing the RADIUS accounting servers with which it shares a secret.
ServerPortNumber	The UDP port it is using to send requests to this server.
RoundTripTime	The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Responses	The number of RADIUS packets received on the accounting port from this server.
MalformedResponses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
BadAuthenticators	The number of RADIUS Accounting-Response packets, which contained invalid authenticators, received from this server.
PendingRequests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.
Timeouts	The number of accounting timeouts to this server. After a timeout it may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
UnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
PacketsDropped	The number of RADIUS packets, which were received from this server on the accounting port and dropped for some other reason.

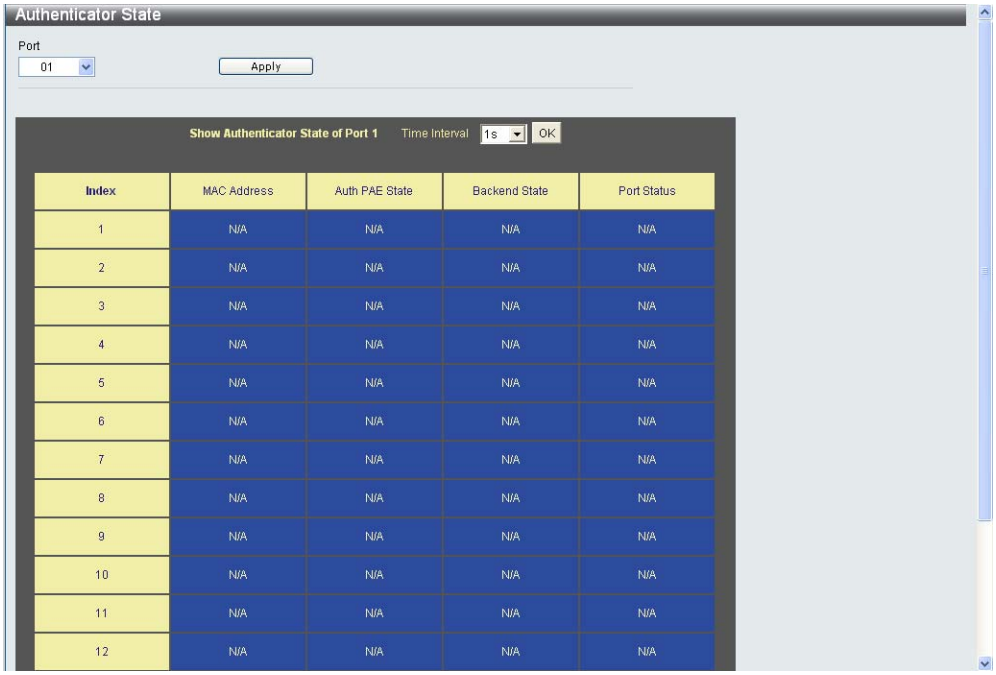
Authenticator State

The following section describes the 802.1X State on the Switch.

To view the **Authenticator State** window for Port-based, click **Monitoring > Port Access Control > Authenticator State**:



To view the **Authenticator State** window for MAC-based, click **Monitoring > Port Access Control > Authenticator State**:



This window displays the Authenticator State for individual ports on a selected device. A polling interval between *1s* and *60s* seconds can be set using the drop-down menu at the top of the window and clicking **OK**.

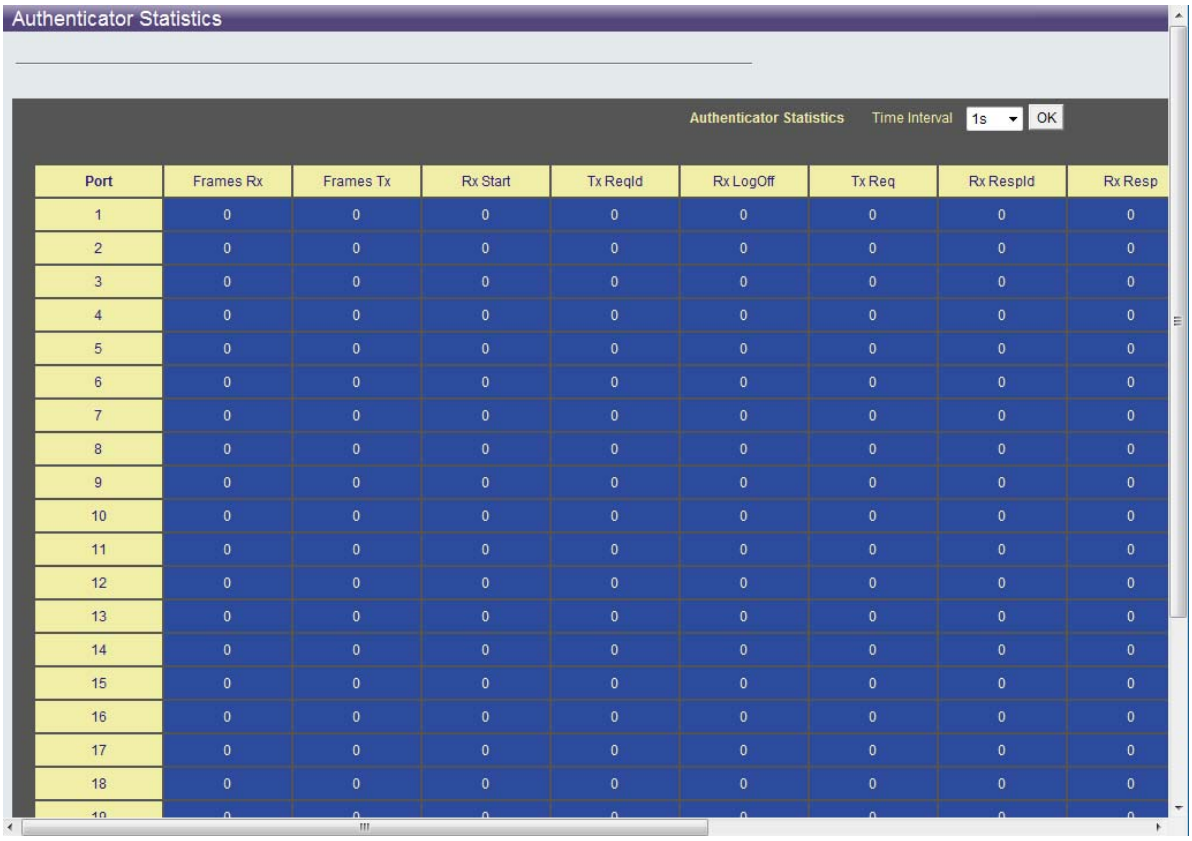
The information on this window is described as follows:

Parameters	Description
MAC Address	The MAC Address of the device of the corresponding index number.
Auth PAE State	The Authenticator PAE State value can be: Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, Force_Auth, Force_Unauth, or N/A. N/A (Not Available) indicates that the port's authenticator capability is disabled.
Backend State	The Backend Authentication State can be Request, Response, Success, Fail, Timeout, Idle, Initialize, or N/A. N/A (Not Available) indicates that the port's authenticator capability is disabled.
Port Status	Controlled Port Status can be Authorized, Unauthorized, or N/A.

Authenticator Statistics

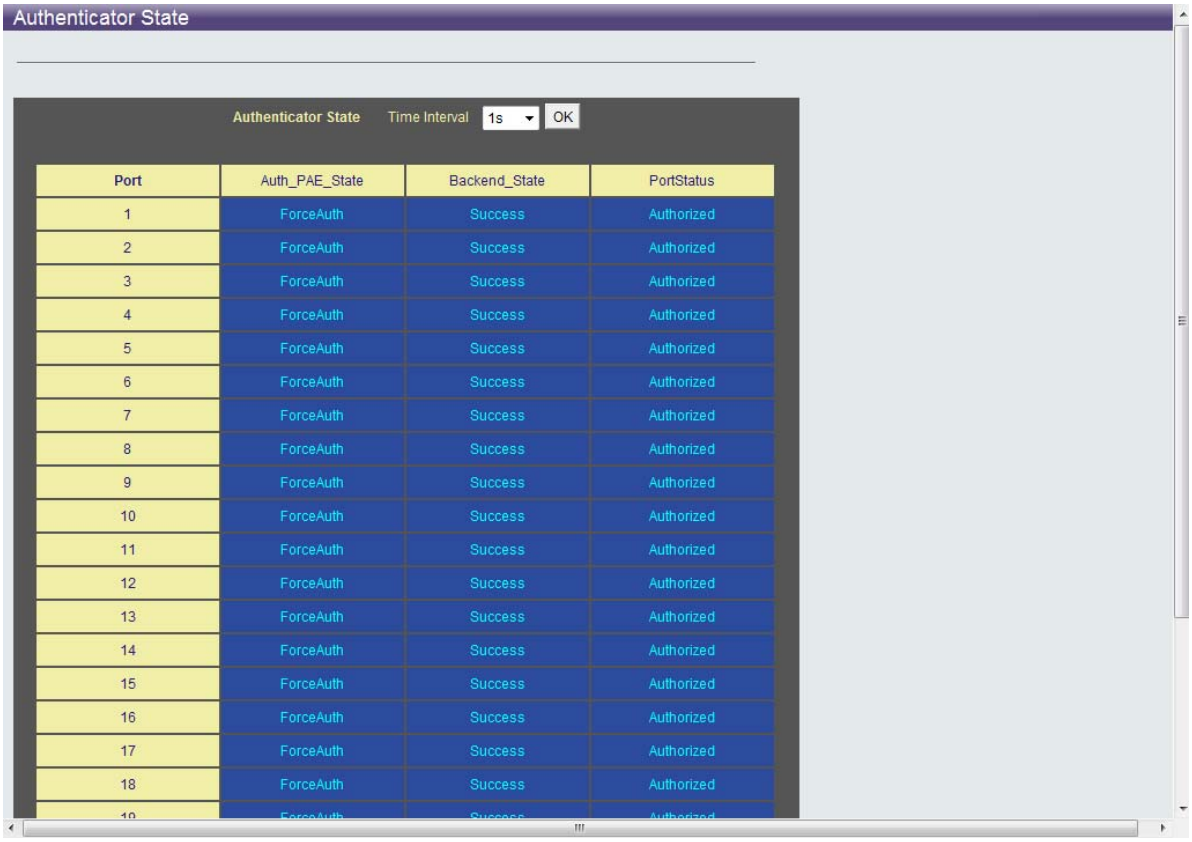
This window contains the statistics objects for the Authenticator PAE associated with each port. An entry appears in this table for each port that supports the Authenticator function.

To view the **Authenticator Statistics** window for Port-based, click **Monitoring > Port Access Control > Authenticator Statistics**:



Port	Frames Rx	Frames Tx	Rx Start	Tx ReqId	Rx LogOff	Tx Req	Rx RespId	Rx Resp
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0

To view the **Authenticator Statistics** window for MAC-based, click **Monitoring > Port Access Control > Authenticator Statistics**:



The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second.

The following fields can be viewed:

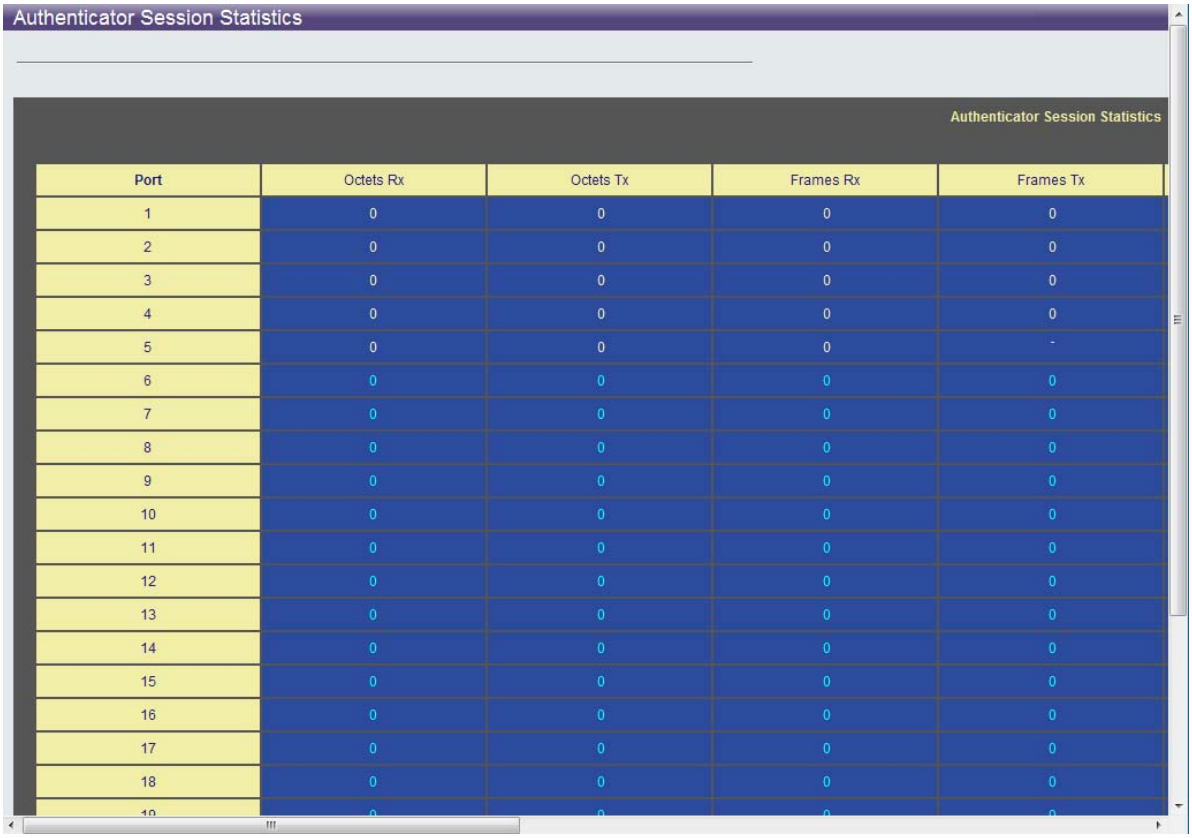
Parameters	Description
Port	The identification number assigned to the Port by the System in which the Port resides.
Frames Rx	The number of valid EAPOL frames that have been received by this Authenticator.
Frames Tx	The number of EAPOL frames that have been transmitted by this Authenticator.
Rx Start	The number of EAPOL Start frames that have been received by this Authenticator.
TxReqId	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
RxLogOff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Tx Req	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
Rx RespId	The number of EAP Resp/Id frames that have been received by this Authenticator.

Parameters	Description
Rx Resp	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx Error	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Last Version	The protocol version number carried in the most recently received EAPOL frame.
Last Source	The source MAC address carried in the most recently received EAPOL frame.

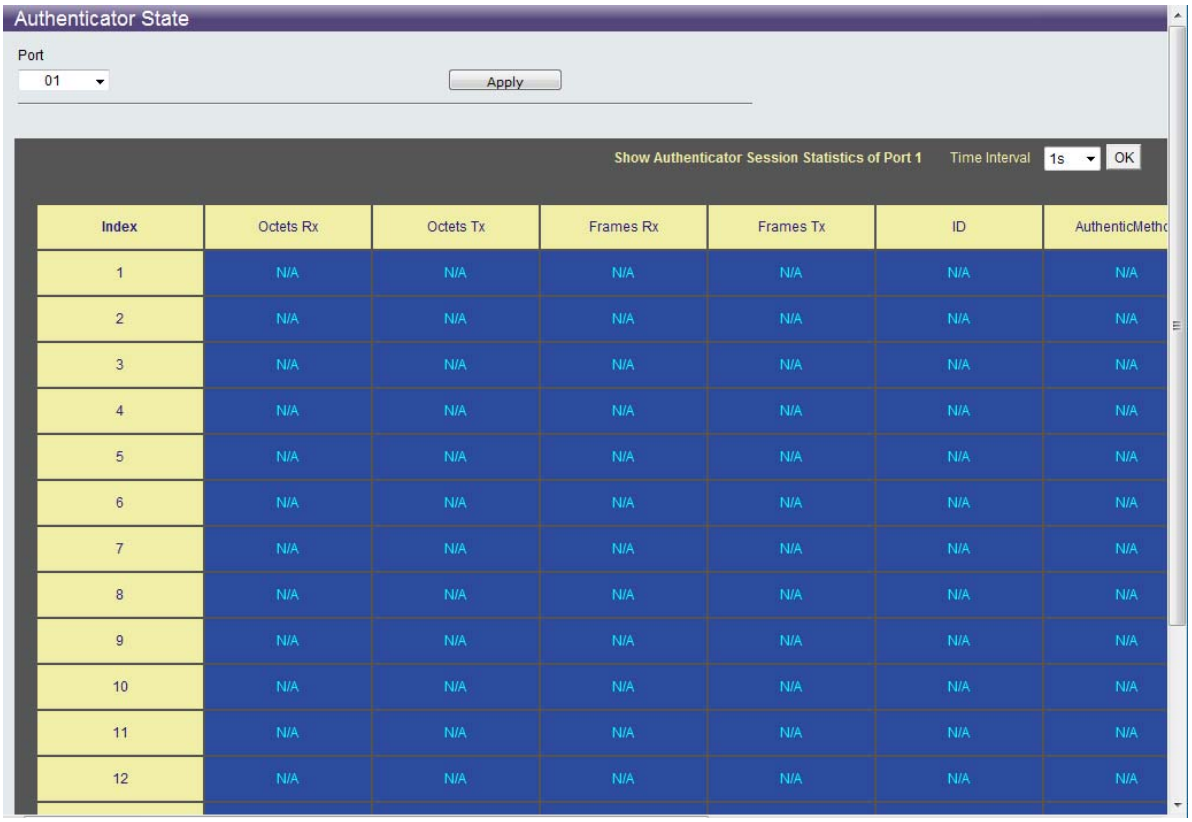
Authenticator Session Statistics

This window contains the session statistics objects for the Authenticator PAE associated with each port. An entry appears in this table for each port that supports the Authenticator function.

To view the **Authenticator Session Statistics** window for Port-based, click **Monitoring > Port Access Control > Authenticator Session Statistics**:



To view the **Authenticator Session Statistics** window for MAC-based, click **Monitoring > Port Access Control > Authenticator Session Statistics**:



The user may select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second.

The following fields can be viewed:

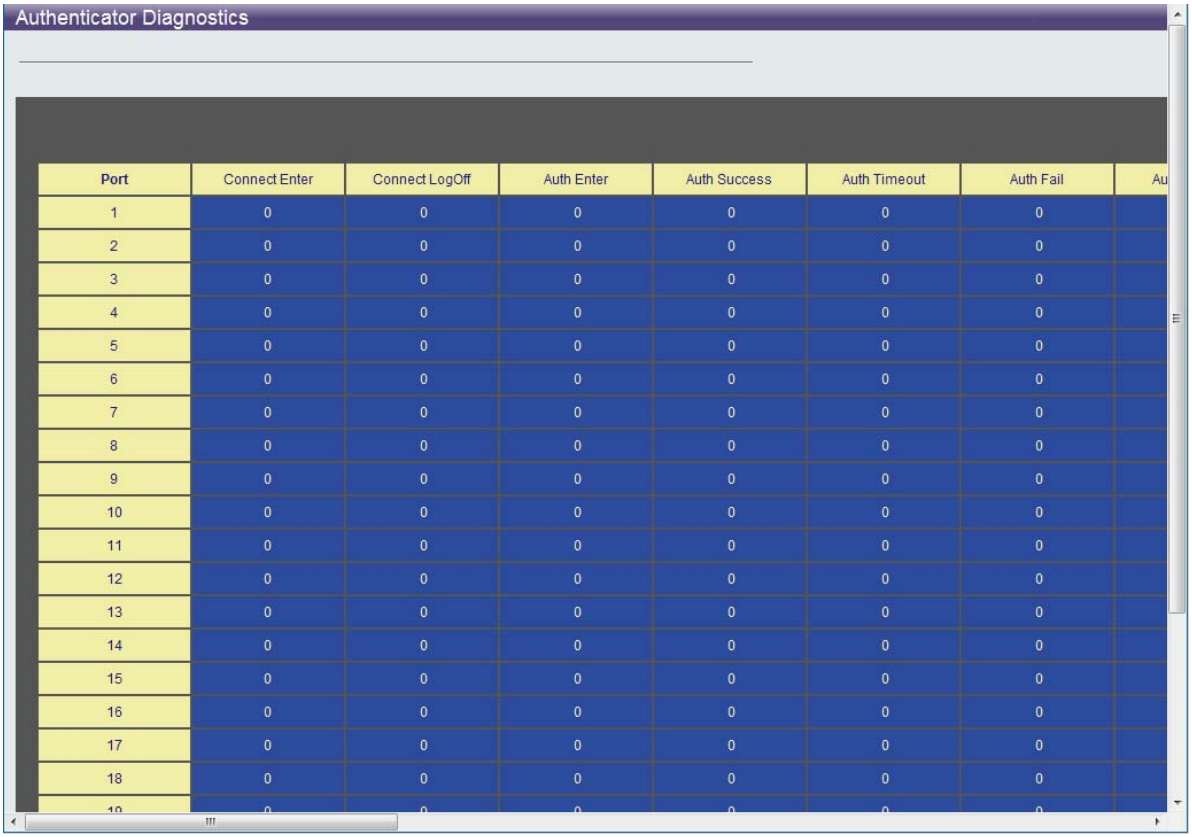
Parameters	Description
Port	The identification number assigned to the Port by the System in which the Port resides.
Octets Rx	The number of octets received in user data frames on this port during the session.
Octets Tx	The number of octets transmitted in user data frames on this port during the session.
Frames Rx	The number of user data frames received on this port during the session.
Frames Tx	The number of user data frames transmitted on this port during the session.
ID	A unique identifier for the session, in the form of a printable ASCII string of at least three characters.
Authentic Method	The authentication method used to establish the session. Valid Authentic Methods include: (1) Remote Authentic Server - The Authentication Server is external to the Authenticator's System. (2) Local Authentic Server - The Authentication Server is located within the Authenticator's System.
Time	The duration of the session in seconds.

Parameters	Description
Terminate Cause	The reason for the session termination. There are eight possible reasons for termination. 1) Supplicant Logoff 2) Port Failure 3) Supplicant Restart 4) Reauthentication Failure 5) AuthControlledPortControl set to ForceUnauthorized 6) Port re-initialization 7) Port Administratively Disabled 8) Not Terminated Yet
UserName	The User-Name representing the identity of the Supplicant PAE.

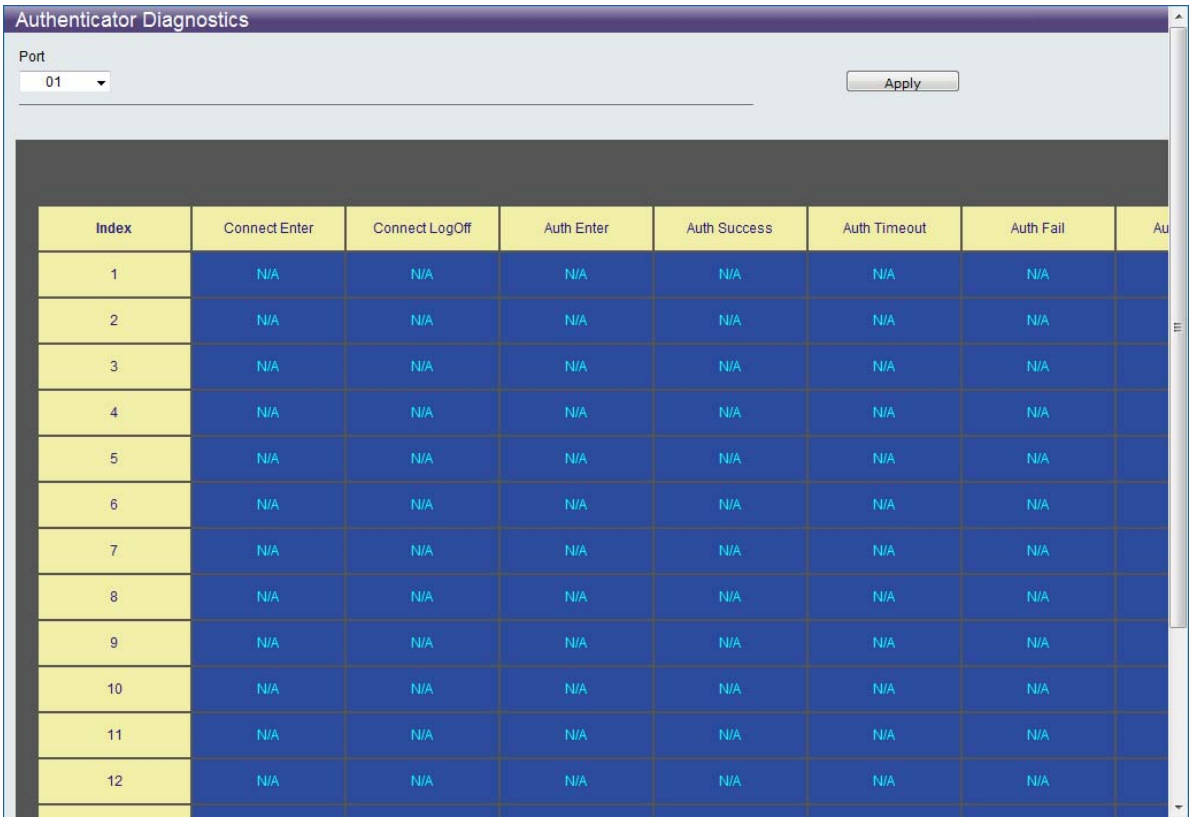
Authenticator Diagnostics

This window contains the diagnostic information regarding the operation of the Authenticator associated with each port. An entry appears in this table for each port that supports the Authenticator function.

To view the **Authenticator Diagnostics** window for Port-based, click **Monitoring > Port Access Control > Authenticator Diagnostics**:



To view the **Authenticator Diagnostics** window for MAC-based, click **Monitoring > Port Access Control > Authenticator Diagnostics**:


Authenticator Diagnostics
Port
01
Apply
Index
Connect Enter
Connect LogOff
Auth Enter
Auth Success
Auth Timeout
Auth Fail
1 N/A N/A N/A N/A N/A N/A
2 N/A N/A N/A N/A N/A N/A
3 N/A N/A N/A N/A N/A N/A
4 N/A N/A N/A N/A N/A N/A
5 N/A N/A N/A N/A N/A N/A
6 N/A N/A N/A N/A N/A N/A
7 N/A N/A N/A N/A N/A N/A
8 N/A N/A N/A N/A N/A N/A
9 N/A N/A N/A N/A N/A N/A
10 N/A N/A N/A N/A N/A N/A
11 N/A N/A N/A N/A N/A N/A
12 N/A N/A N/A N/A N/A N/A

The following fields can be viewed:

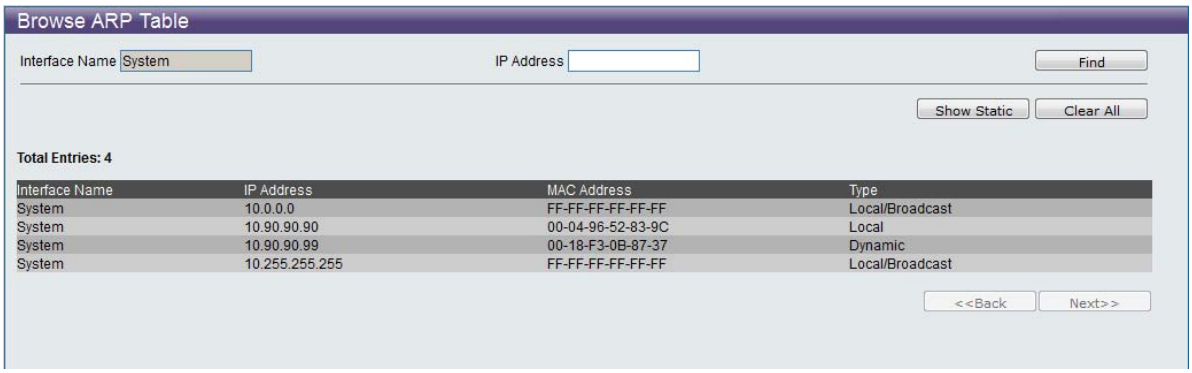
Parameters	Description
Port	The identification number assigned to the Port by the System in which the Port resides.
Connect Enter	Counts the number of times that the state machine transitions to the CONNECTING state from any other state.
Connect LogOff	Counts the number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.
Auth Enter	Counts the number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAP-Response/ Identity message being received from the Supplicant.
Auth Success	Counts the number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant (authSuccess = TRUE).
Auth Timeout	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout (authTimeout = TRUE).
Auth Fail	Counts the number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure (authFail = TRUE).

Parameters	Description
Auth Reauth	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a reauthentication request (reAuthenticate = TRUE).
Auth Start	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.
Auth LogOff	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
Authed Reauth	Counts the number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a reauthentication request (reAuthenticate = TRUE).
Authed Start	Counts the number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant.
Authed LogOff	Counts the number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOL-Logoff message being received from the Supplicant.
Responses	Counts the number of times that the state machine sends an initial Access-Request packet to the Authentication server (i.e., executes sendRespToServer on entry to the RESPONSE state). Indicates that the Authenticator attempted communication with the Authentication Server.
AccessChallenges	Counts the number of times that the state machine receives an initial Access-Challenge packet from the Authentication server (i.e., aReq becomes TRUE, causing exit from the RESPONSE state). Indicates that the Authentication Server has communication with the Authenticator.
OtherReqToSupp	Counts the number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure, or Success message) to the Supplicant (i.e., executes txReq on entry to the REQUEST state). Indicates that the Authenticator chose an EAP-method.
NonNakRespFromSup	Counts the number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK (i.e., rxResp becomes TRUE, causing the state machine to transition from REQUEST to RESPONSE, and the response is not an EAP-NAK). Indicates that the Supplicant can respond to the Authenticator's chosen EAP-method.
Bac Auth Success	Counts the number of times that the state machine receives an Accept message from the Authentication Server (i.e., aSuccess becomes TRUE, causing a transition from RESPONSE to SUCCESS). Indicates that the Supplicant has successfully authenticated to the Authentication Server.
Bac Auth Fail	Counts the number of times that the state machine receives a Reject message from the Authentication Server (i.e., aFail becomes TRUE, causing a transition from RESPONSE to FAIL). Indicates that the Supplicant has not authenticated to the Authentication Server.

Browse ARP Table

This window displays current ARP entries on the Switch. To search a specific ARP entry, enter an Interface Name or an IP Address at the top of the window and click **Find**. Click the **Show Static** button to display static ARP table entries. To clear the ARP Table, click **Clear All**.

The view this window, click **Monitoring > Browse ARP Table**:



Click on the **Find** button to find a specific entry based on the parameters entered.

Click on the **Show Static** button to display all the static entries.

Click on the **Clear All** button to clear all the entered data from the fields.

Browse VLAN

This window allows the VLAN status for each of the Switch's ports to be viewed by VLAN. Enter a VID (VLAN ID) in the field at the top of the window and click the **Find** button.

To view this window, click **Monitoring > Browse VLAN**:

Browse VLAN
VID
Find
VLAN ID: 1
VLAN Name: default
VLAN Type: Static
Advertisement: Enabled
Total Entries: 1
Port
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
U U U U U U U U U U U U U U U U U U U U U U U U
<<Back
Next>>
Note: T: Tagged Port , U: Untagged Port, F: Forbidden Port,

Click on the **Find** button to find a specific entry based on the parameters entered.

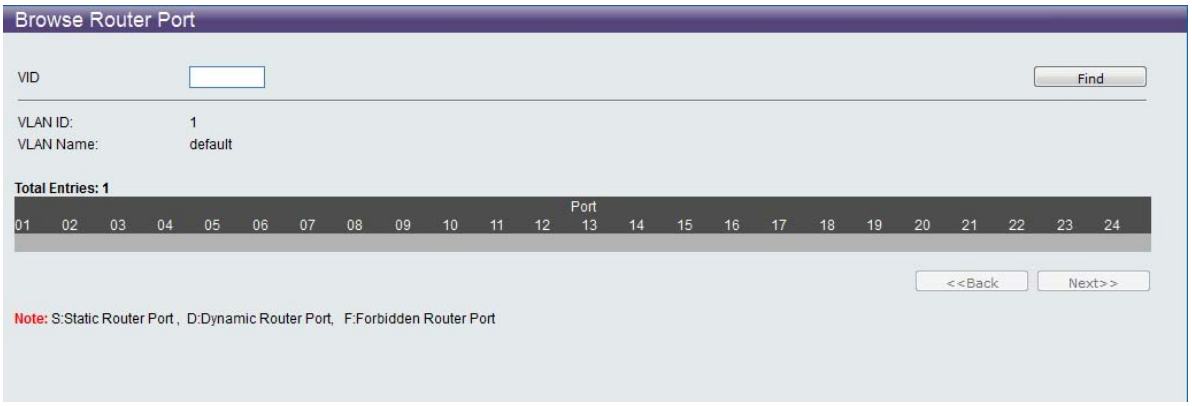
IGMP Snooping Folder

The following windows are used to configure the IGMP Snooping settings of the Switch.

Browse IGMP Router Port

This window displays which of the Switch's ports are currently configured as router ports. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by S. A router port that is dynamically configured by the Switch is designated by D, while a Forbidden port is designated by F. Enter a VID (VLAN ID) in the field at the top of the window and click the **Find** button to display the various types of IGMP router ports that belong to the specified VLAN.

To view this window, click **Monitoring > IGMP Snooping > Browse IGMP Router Port:**

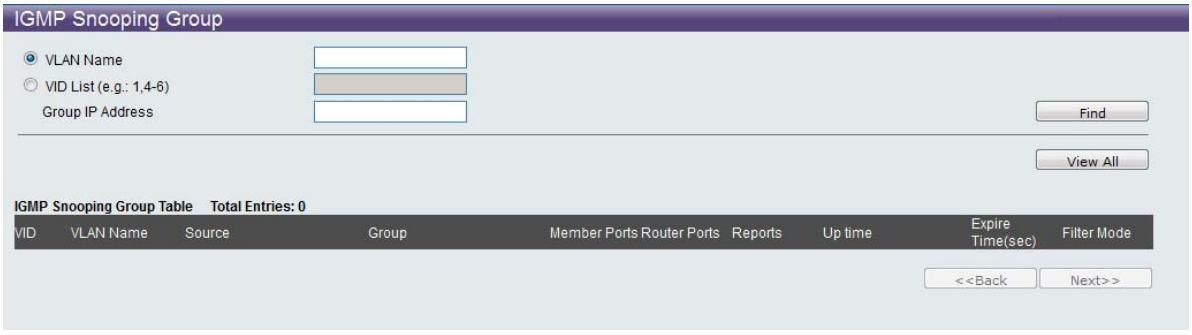

Browse Router Port
VID
Find
VLAN ID: 1
VLAN Name: default
Total Entries: 1
Port
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
<<Back
Next>>
Note: S:Static Router Port , D:Dynamic Router Port, F:Forbidden Router Port

Click on the **Find** button to find a specific entry based on the parameters entered.

IGMP Snooping Group

This window allows the Switch's IGMP Snooping Group Table to be searched. IGMP snooping allows the Switch to read the Multicast Group IP address and source IP address from IGMP packets that pass through the Switch. The number of IGMP reports that are snooped are displayed in the Reports field.

To view this window, click **Monitoring > IGMP Snooping > IGMP Snooping Group:**


IGMP Snooping Group
VLAN Name
VID List (e.g.: 1,4-6)
Group IP Address
Find
View All
IGMP Snooping Group Table Total Entries: 0
VID VLAN Name Source Group Member Ports Router Ports Reports Up time Expire Time(sec) Filter Mode
<<Back
Next>>

In this window, the following parameters can be configured:

Parameters	Description
VLAN Name	The VLAN ID of the multicast group.
VID List (e.g.: 1, 4-6)	The VLAN ports of the multicast group.
Group IP Address	The IP address of the multicast group.

Click on the **Find** button to find a specific entry based on the parameters entered.

Click on the **View All** button to view all the existing entries.

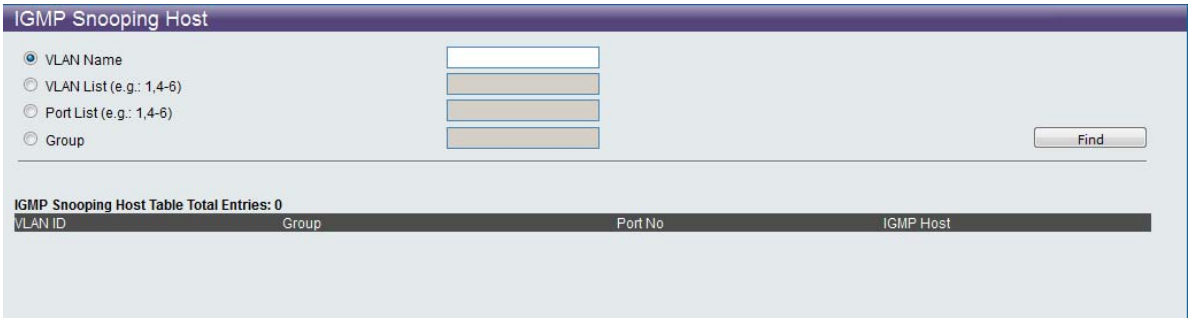
NOTE

To configure IGMP snooping for the Switch, go to the **L2 Features** folder and select **IGMP Snooping > IGMP Snooping Settings**.

IGMP Snooping Host

This window displays current IGMP Snooping host information on the Switch.

To view this window, click **Monitoring > IGMP Snooping > IGMP Snooping Host:**



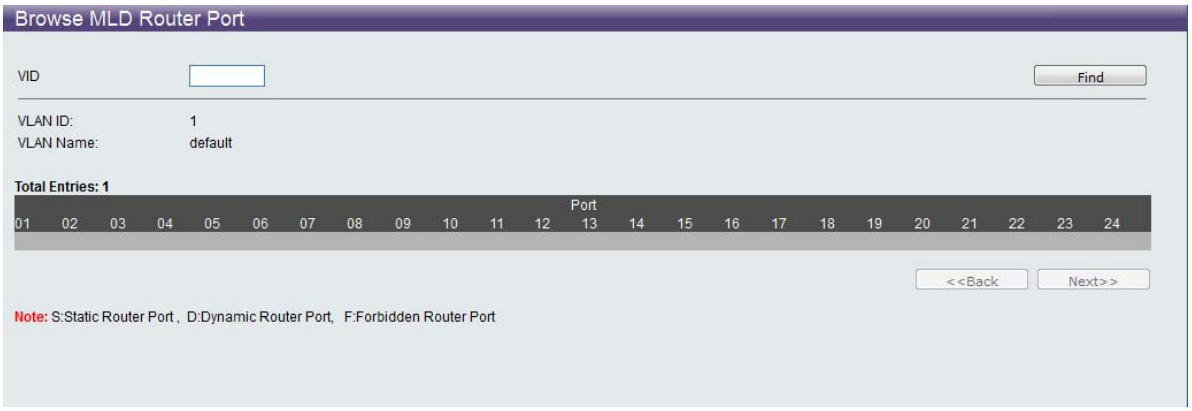
Click the corresponding radio button, enter the VLAN Name, VLAN List, Port List, or the Group to view IGMP snooping host information, and click **Find**. The searched entries will be displayed in the lower half of the window.

MLD Snooping Folder

Browse MLD Router Port

This window displays which of the Switch's ports are currently configured as router ports in IPv6. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by S. A router port that is dynamically configured by the Switch and is designated by D, whereas a Forbidden port is designated by F. Enter a VID (VLAN ID) in the field at the top of the window and click the **Find** button to display the various types of MLD router ports that beliong to the specified VLAN.

To view this window, click **Monitoring > MLD Snooping > Browse MLD Router Port:**


Browse MLD Router Port
VID
Find
VLAN ID: 1
VLAN Name: default
Total Entries: 1
Port
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
<<Back
Next>>
Note: S:Static Router Port , D:Dynamic Router Port, F:Forbidden Router Port

MLD Snooping Group

The following window allows the user to view MLD Snooping Groups present on the Switch. MLD Snooping is an IPv6 function comparable to IGMP Snooping for IPv4.

To view this window, click **Monitoring > MLD Snooping > MLD Snooping Group:**

Click on the **Find** button to find a specific entry based on the parameters entered.

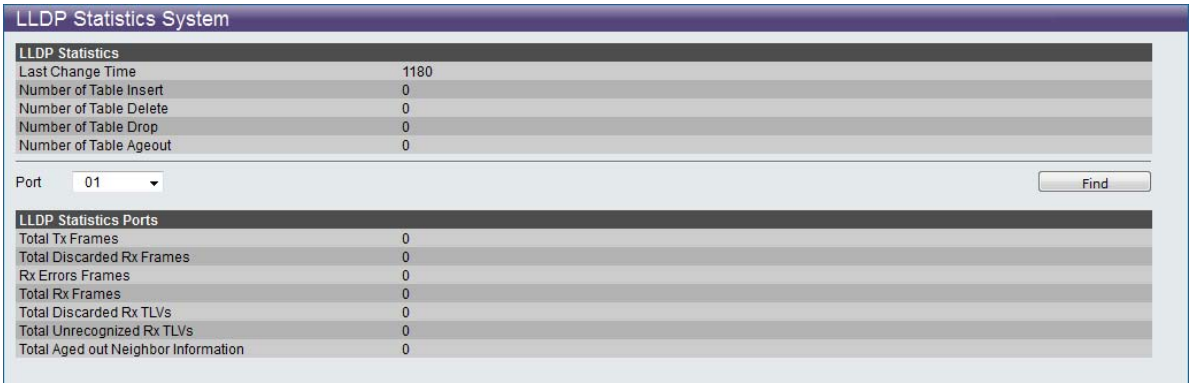
Click on the **View All** button to view all the existing entries.

LLDP Folder

The Switch offers three LLDP statistic windows.

LLDP Statistics System

To view this window, click **Monitoring > LLDP > LLDP Statistics System**:


LLDP Statistics System
LLDP Statistics
Last Change Time 1180
Number of Table Insert 0
Number of Table Delete 0
Number of Table Drop 0
Number of Table Ageout 0
Port 01
Find
LLDP Statistics Ports
Total Tx Frames 0
Total Discarded Rx Frames 0
Rx Errors Frames 0
Total Rx Frames 0
Total Discarded Rx TLVs 0
Total Unrecognized Rx TLVs 0
Total Aged out Neighbor Information 0

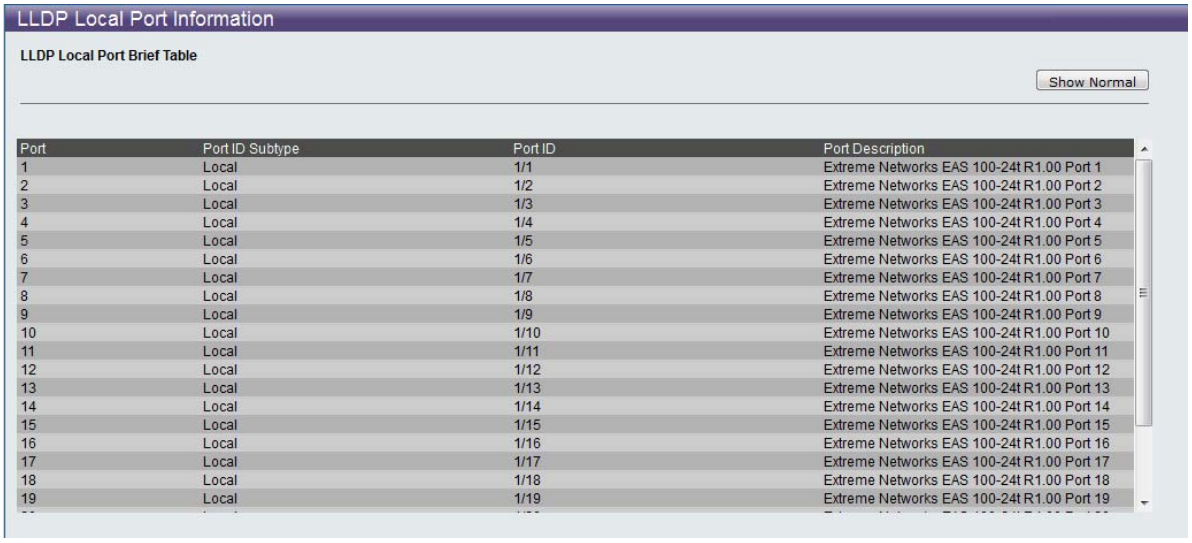
In this window, the following parameters can be configured:

Parameters	Description
Port	Specifies the port to be used for this configuration.

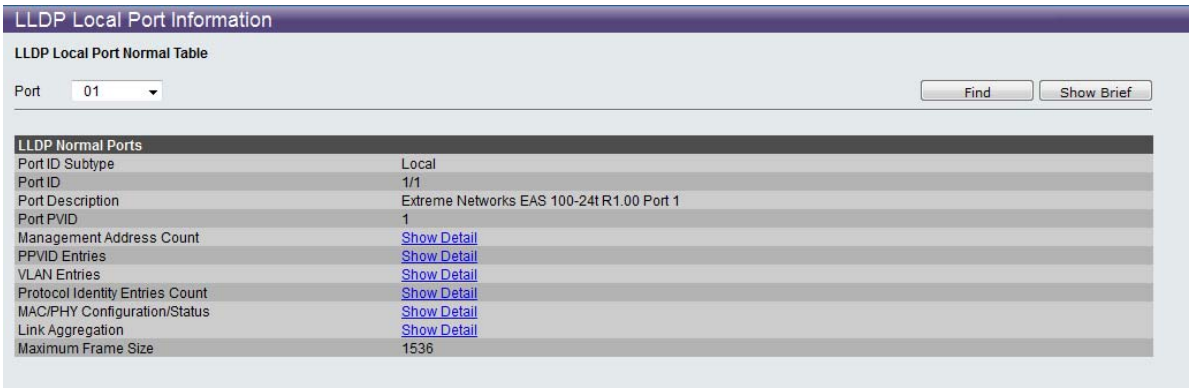
Click on the **Find** button to find a specific entry based on the parameters entered.

LLDP Local Port Information

To view this window, click **Monitoring > LLDP > LLDP Local Port Information:**


LLDP Local Port Information
LLDP Local Port Brief Table
Show Normal
Port Port ID Subtype Port ID Port Description
1 Local 1/1 Extreme Networks EAS 100-24t R1.00 Port 1
2 Local 1/2 Extreme Networks EAS 100-24t R1.00 Port 2
3 Local 1/3 Extreme Networks EAS 100-24t R1.00 Port 3
4 Local 1/4 Extreme Networks EAS 100-24t R1.00 Port 4
5 Local 1/5 Extreme Networks EAS 100-24t R1.00 Port 5
6 Local 1/6 Extreme Networks EAS 100-24t R1.00 Port 6
7 Local 1/7 Extreme Networks EAS 100-24t R1.00 Port 7
8 Local 1/8 Extreme Networks EAS 100-24t R1.00 Port 8
9 Local 1/9 Extreme Networks EAS 100-24t R1.00 Port 9
10 Local 1/10 Extreme Networks EAS 100-24t R1.00 Port 10
11 Local 1/11 Extreme Networks EAS 100-24t R1.00 Port 11
12 Local 1/12 Extreme Networks EAS 100-24t R1.00 Port 12
13 Local 1/13 Extreme Networks EAS 100-24t R1.00 Port 13
14 Local 1/14 Extreme Networks EAS 100-24t R1.00 Port 14
15 Local 1/15 Extreme Networks EAS 100-24t R1.00 Port 15
16 Local 1/16 Extreme Networks EAS 100-24t R1.00 Port 16
17 Local 1/17 Extreme Networks EAS 100-24t R1.00 Port 17
18 Local 1/18 Extreme Networks EAS 100-24t R1.00 Port 18
19 Local 1/19 Extreme Networks EAS 100-24t R1.00 Port 19

After clicking the **Show Normal** button, the following window will appear:



In this window, the following parameters can be configured:

Parameters	Description
Port	Specifies the port to be used for this configuration.

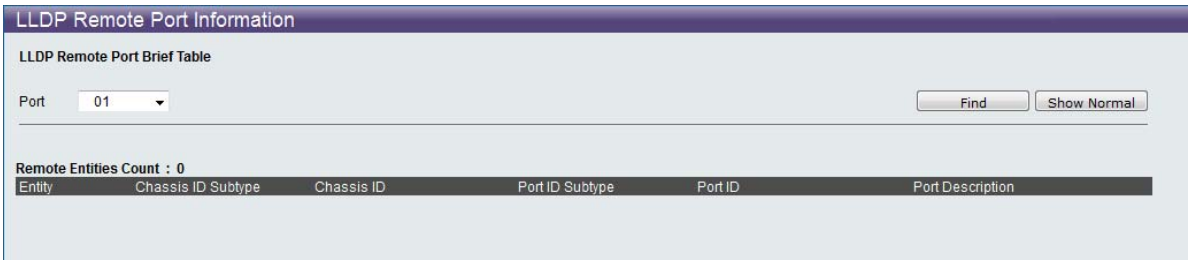
To find the specific entry entered, click on the **Find** button.

To view the brief display for the selected port, click on the **Show Brief** button.

In this window the user can view detailed information for each individual category listed by clicking on the **Show Detail** link next to it.

LLDP Remote Port Information

To view this window, click **Monitoring > LLDP > LLDP Remote Port Information:**



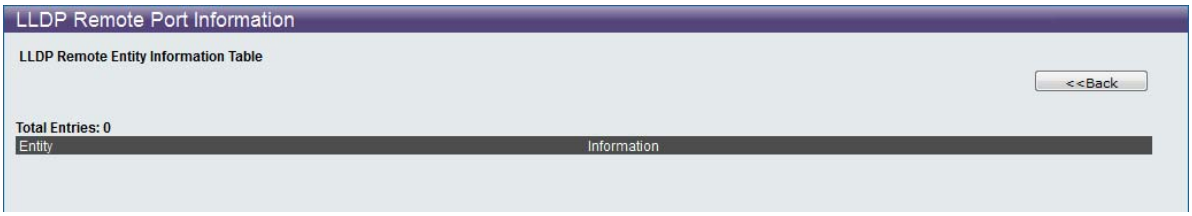
In this window, the following parameters can be configured:

Parameters	Description
Port	Specifies the port to be used for this configuration.

To find the specific entry entered, click on the **Find** button.

To view the normal display for the selected port, click on the **Show Normal** button.

After clicking the **Show Normal** button, the following window will appear:



MBA Authentication State

To view the MBA Authentication State window, click **Monitoring > MBA Authentication State:**

In this window, the following parameters can be configured:

Parameters	Description
Port List	Specifies the list of port to be used for this configuration.

To find the specific entry entered, click on the **Find** button.

To clear by port, click on the **Clear By Port** button.

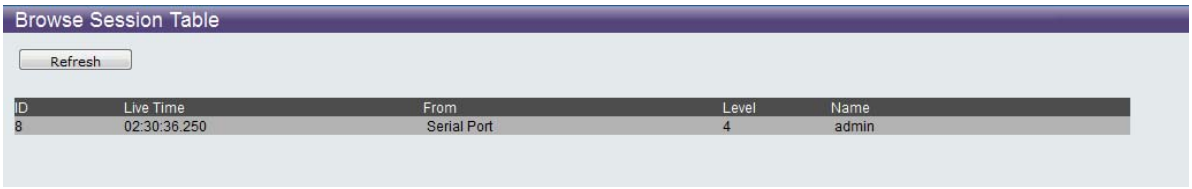
To view all the MBA Authentication hosts, click on the **View All Hosts** button.

To clear all the MBA Authentication hosts, click on the **Clear All Hosts** button.

Browse Session Table

This window displays the management sessions since the Switch was last rebooted.

To view the Browse Session Table window, click **Monitoring > Browse Session Table:**

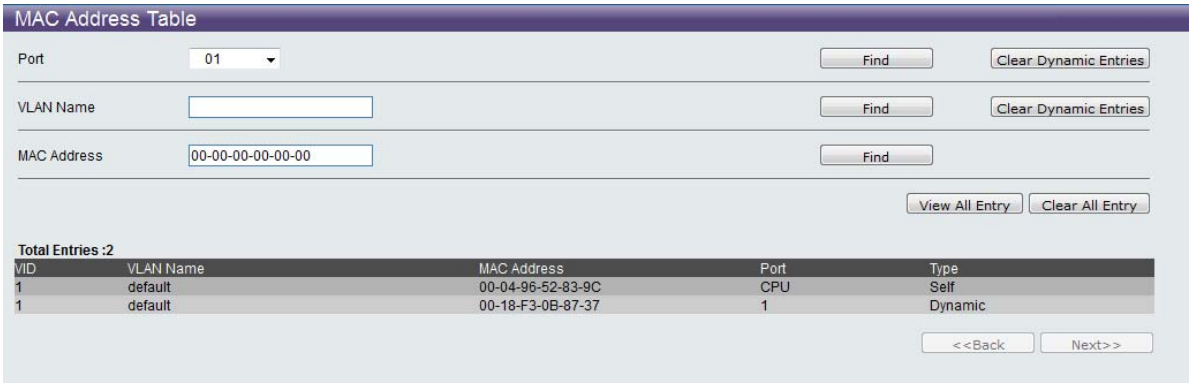


Click on the **Refresh** button to refresh the display list.

MAC Address Table

This allows the Switch's dynamic MAC address forwarding table to be viewed. When the Switch learns an association between a MAC address and a port number, it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch.

To view the MAC Address Table window, click **Monitoring > MAC Address Table:**



In this window, the following parameters can be configured:

Parameters	Description
Port	The port to which the MAC address below corresponds.
VLAN Name	Enter a VLAN Name for the forwarding table to be browsed by.
MAC Address	Enter a MAC address for the forwarding table to be browsed by.
Find	Allows the user to move to a sector of the database corresponding to a user defined port, VLAN, or MAC address.
Clear Dynamic Entries	Click this button will allow the user to delete all dynamic entries of the address table.
View All Entry	Click this button will allow the user to view all entries of the address table.
Clear All Entry	Click this button will allow the user to delete all entries of the address table.

Click on the **Find** button to find a specific entry based on the parameters entered.

Click on the **Clear Dynamic Entries** button to clear all the dynamic entries.

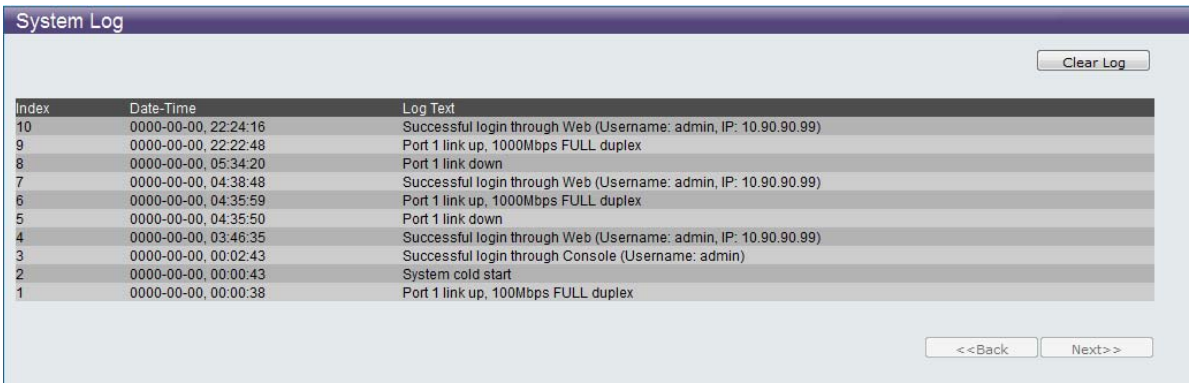
Click on the **View All Entry** button to view all the entries available.

Click on the **Clear All Entry** button to clear all the entries displayed.

System Log

The web manager allows the Switch's history log, as compiled by the Switch's management agent, to be viewed.

To view the Switch history log, click **Monitoring > System Log**:



The Switch can record event information in its own logs. Click **Next** to go to the next page of the **System Log** window. Clicking **Clear** will allow the user to clear the Switch History Log.

In this window, the following parameters can be configured:

Parameters	Description
Index	A counter incremented whenever an entry to the Switch's history log is made. The table displays the last entry (highest sequence number) first.
Date-Time	Displays the time in days, hours, minutes, and seconds since the Switch was last restarted.
Log Text	Displays text describing the event that triggered the history log entry.

8 Save and Tools

CHAPTER

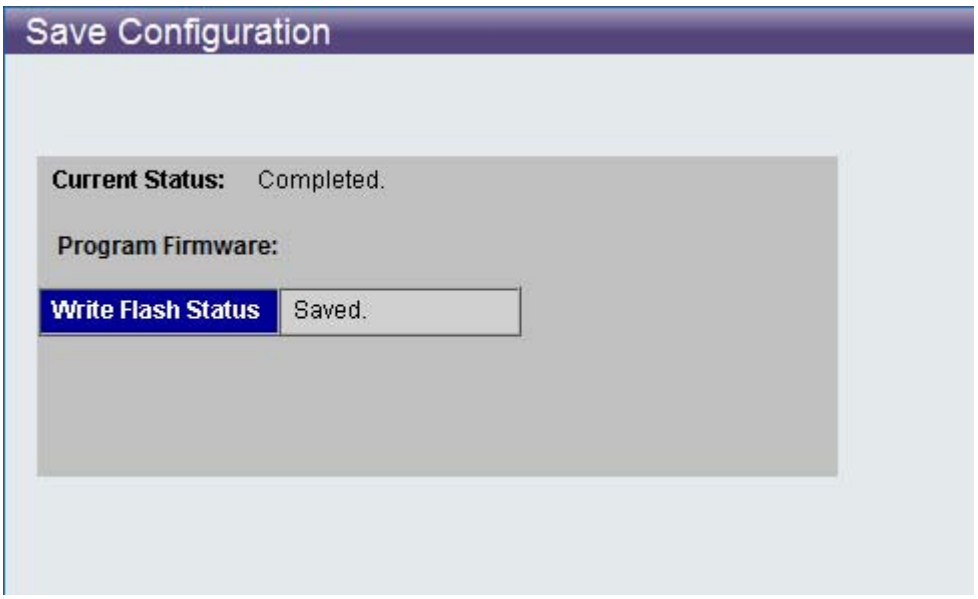
The three **Save** windows include: **Save Configuration**, **Save Log**, and **Save All**. Each version of the window will aid the user in saving configurations to the Switch's memory.

The options include:

- **Save Configuration** to save the current configuration file.
- **Save Log** to save only the current log.
- **Save All** to save the current configuration file and log.

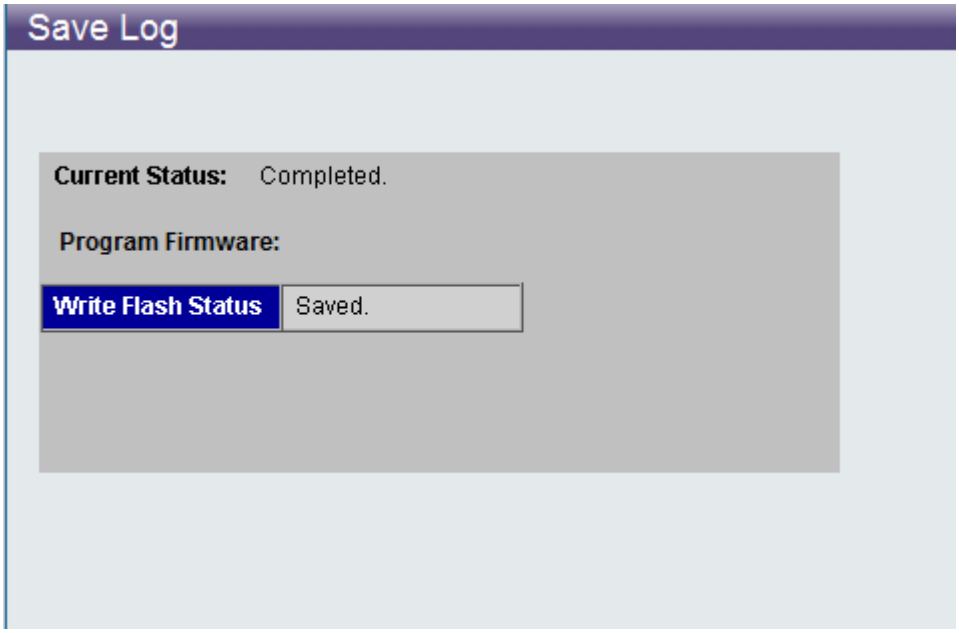
Save Configuration

Open the **Save** drop-down menu at the top of the Web manager and click **Save Configuration** to open the following window:



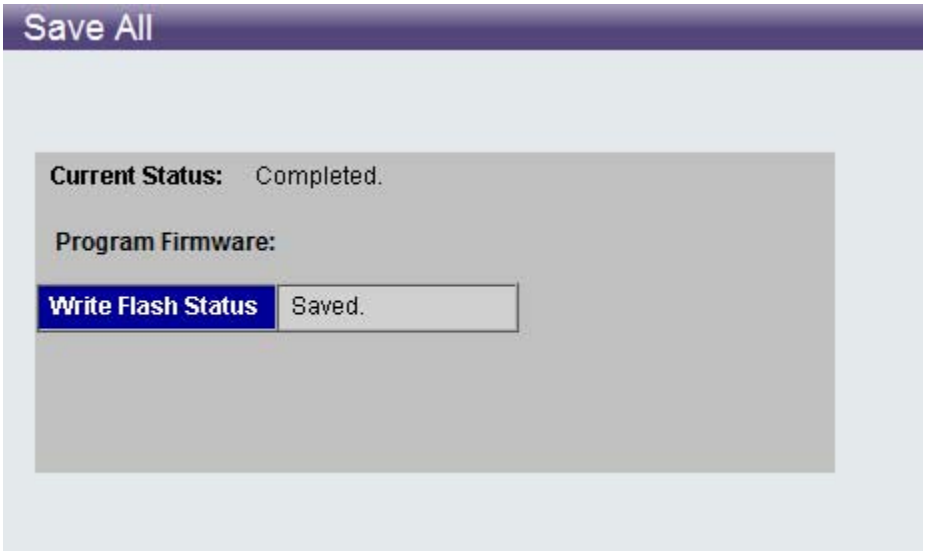
Save Log

Open the **Save** drop-down menu at the top of the Web manager and click **Save Log** to open the following window:



Save All

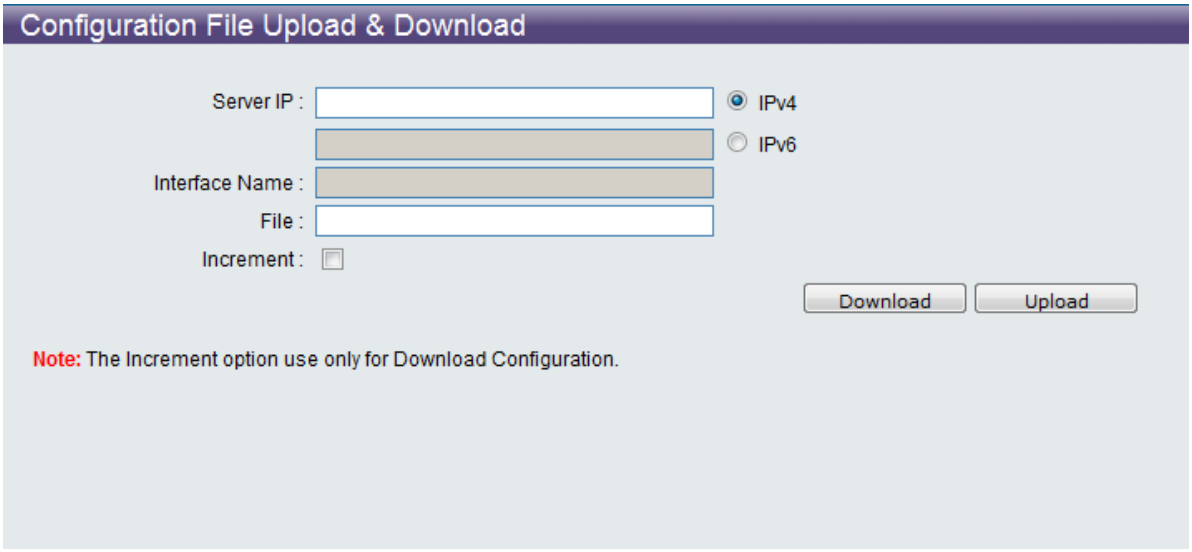
Open the **Save** drop-down menu at the top of the Web manager and click **Save All** to open the following window:



Configuration File Upload & Download

The Switch can upload and download configuration files.

Open the **Tools** drop-down menu on the left-hand side of the menu bar at the top of the Web manager and click **Configuration File Upload & Download** to open the following window:

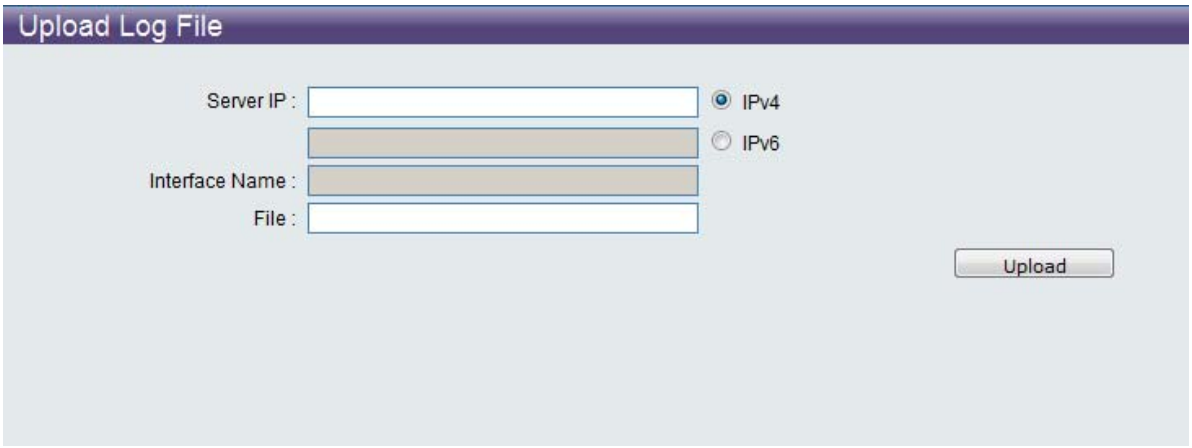


Use the radio button to select IPv4 and specify File name or use the radio button to select IPv6, enter a Server IP, Interface Name, and File name. Click either **Download** or **Upload** to initiate the file transfer.

Upload Log File

To upload a log file, enter a Server IP address, use the radio button to select IPv4 and then enter a File name, or use the radio button to select IPv6, enter a Server IP, Interface Name, and File name. Click **Upload**.

Open the **Tools** drop-down menu on the left-hand side of the menu bar at the top of the Web manager and click **Upload Log File** to open the following window:



Reset

The Reset function has several options when resetting the Switch. Some of the current configuration parameters can be retained while resetting all other configuration parameters to their factory defaults.

NOTE

Only the Reset System option will enter the factory default parameters into the Switch's non-volatile RAM, and then restart the Switch. All other options enter the factory defaults into the current configuration, but do not save this configuration. Reset System will return the Switch's configuration to the state it was when it left the factory.

Reset gives the option of retaining the Switch's User Accounts and History Log while resetting all other configuration parameters to their factory defaults. If the Switch is reset using this window, and **Save Changes** is not executed, the Switch will return to the last saved configuration when rebooted.

Open the **Tools** drop-down menu on the left-hand side of the menu bar at the top of the Web manager and click **Reset System** to open the following window:

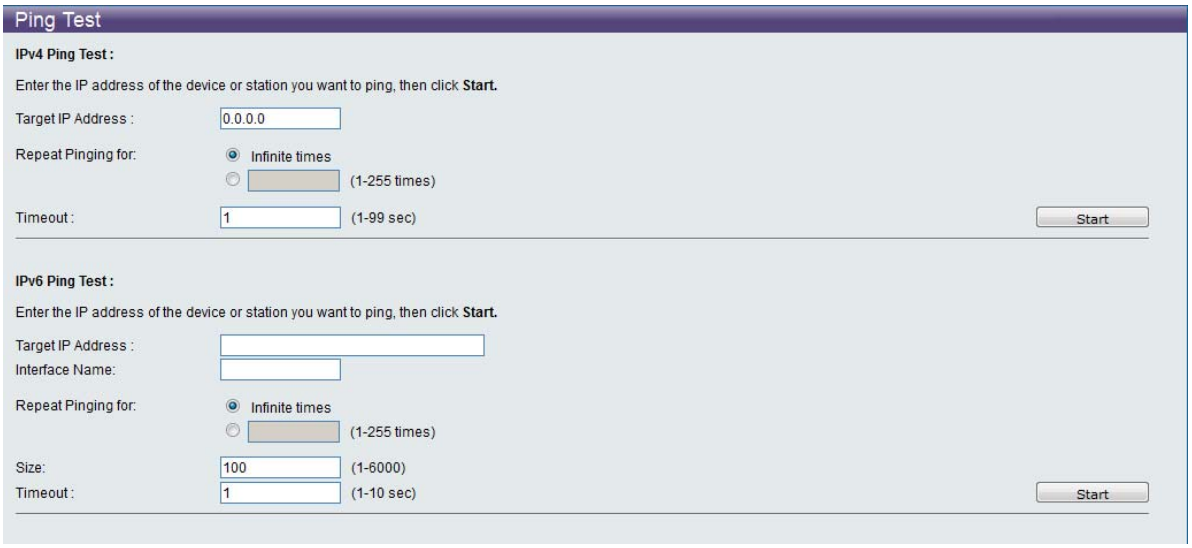
Reset System
Reset
Reset Config
Reset System
Proceed with system reset except IP address, log, user account and banner.
Switch will be reset to factory defaults.
Switch will be reset to factory defaults and reboot.
Apply

Click on the **Apply** button to accept the changes made.

Ping Test

Users can Ping either an IPv4 address or an IPv6 address. Ping is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or “echoes” the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

Open the **Tools** drop-down menu on the left-hand side of the menu bar at the top of the Web manager and click **Ping Test** to open the following window:



You may click the Infinite times radio button, in the **Repeat Pinging for** field, which will tell the ping program to keep sending ICMP Echo packets to the specified IP address until the program is stopped. The user may opt to choose a specific number of times to ping the Target IP Address by clicking its radio button and entering a number between *1* and *255*. Click **Start** to initiate the Ping program.

In this window, the following parameters can be configured:

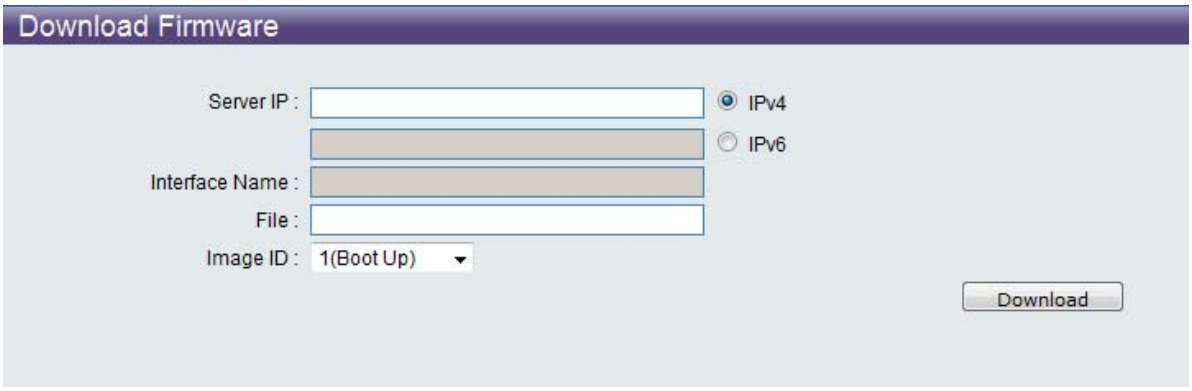
Parameter	Description
Target IP Address	Enter an IP address to be Pinged.
Interface Name	For IPv6 only, enter the name of the interface to be Pinged.
Repeat Pinging for	Enter the number of times desired to attempt to Ping either the IPv4 address or the IPv6 address configured in this window. Users may enter a number of times between *1* and *255*.
Size	For IPv6 only, enter a value between *1* and *6000*. The default is *100*.
Timeout	For IPv4, select a timeout period between *1* and *99* seconds for this Ping message to reach its destination. For IPv6, select a timeout period between *1* and *10* seconds for this Ping message to reach its destination. In either case, if the packet fails to find the IP address in this specified time, the Ping packet will be dropped.

Click **Start** to initialize the Ping program.

Download Firmware

The Switch supports dual image storage for firmware file backup and restoration. The firmware images are indexed by ID number 1 or 2. To change the boot firmware image, use the Image ID drop-down menu to select the desired firmware file to backup or restore. The default Switch settings will use image ID 1 as the boot firmware file.

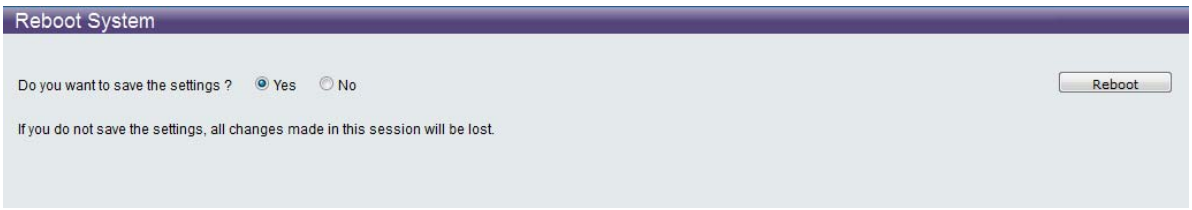
Open the **Tools** drop-down menu on the left-hand side of the menu bar at the top of the Web manager and click **Download Firmware** to open the following window:



Use the radio button to select either IPv4 or IPv6. Enter the TFTP Server IP address for the type of IP selected. Specify the path/file name of the TFTP File. Select the desired Image ID, *1(Boot Up)* or *2*. Click **Download** to initiate the file transfer.

Reboot System

The following window is used to restart the Switch.


Reboot System
Do you want to save the settings ?
Yes
No
Reboot
If you do not save the settings, all changes made in this session will be lost.

Clicking the Yes radio button will instruct the Switch to save the current configuration to non-volatile RAM before restarting the Switch.

Clicking the No radio button instructs the Switch not to save the current configuration before restarting the Switch. All of the configuration information entered from the last time **Save Changes** was executed will be lost.

Click the **Reboot** button to restart the Switch.

APPENDIX A

System Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this Switch.

Category	Event Description	Log Content	Severity
System	System cold start	System cold start	Critical
	System warm start	System warm start	Critical
	Configuration saved to flash	Configuration saved to flash (Username: <username>, IP: <ipaddr>)	Informational
	Configuration saved to flash by console	Configuration saved to flash by console (Username: <username>)	Informational
	System log saved to flash	System log saved to flash (Username: <username>, IP: <ipaddr>)	Informational
	System log saved to flash by console	System log saved to flash by console (Username: <username>)	Informational
	Configuration and log saved to flash	Configuration and log saved to flash (Username: <username>, IP: <ipaddr>)	Informational
	Configuration and log saved to flash by console	Configuration and log saved to flash by console (Username: <username>)	Informational
Upload/Download	Firmware upgraded successfully	Firmware upgraded successfully (Username: <username>, IP: <ipaddr>)	Informational
	Firmware upgraded by console successfully	Firmware upgraded by console successfully (Username: <username>)	Informational
	Firmware upgrade was unsuccessful	Firmware upgrade was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning
	Firmware upgrade by console was unsuccessful	Firmware upgrade by console was unsuccessful! (Username: <username>)	Warning
	Configuration successfully downloaded	Configuration successfully downloaded (Username: <username>, IP: <ipaddr>)	Informational
	Configuration successfully downloaded by console	Configuration successfully by console downloaded(Username: <username>)	Informational

Category	Event Description	Log Content	Severity
	Configuration download was unsuccessful	Configuration download was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning
	Configuration download by console was unsuccessful	Configuration download by console was unsuccessful! (Username: <username>)	Warning
	Configuration successfully uploaded	Configuration successfully uploaded (Username: <username>, IP: <ipaddr>)	Informational
	Configuration successfully uploaded by console	Configuration successfully by console uploaded (Username: <username>)	Informational
	Configuration upload was unsuccessful	Configuration upload was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning
	Configuration upload by console was unsuccessful	Configuration upload by console was unsuccessful! (Username: <username>)	Warning
	Log message successfully uploaded	Log message successfully uploaded (Username: <username>, IP: <ipaddr>)	Informational
	Log message successfully uploaded by console	Log message successfully by console uploaded (Username: <username>)	Informational
	Log message upload was unsuccessful	Log message upload was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning
	Log message upload by console was unsuccessful	Log message upload by console was unsuccessful! (Username: <username>)	Warning
Interface	Port link up	Port <portNum> link up, <link state>	Informational
	Port link down	Port <portNum> link down	Informational
Console	Successful login through Console	Successful login through Console (Username: <username>)	Informational
	Login failed through Console	Login failed through Console (Username: <username>)	Warning
	Logout through Console	Logout through Console (Username: <username>)	Informational
	Console session timed out	Console session timed out (Username: <username>)	Informational
Web	Successful login through Web	Successful login through Web (Username: <username>, IP: <ipaddr>)	Informational
	Login failed through Web	Login failed through Web (Username: <username>, IP: <ipaddr>)	Warning
	Logout through Web	Logout through Web (Username: <username>, IP: <ipaddr>)	Informational
	Web session timed out	Web session timed out (Username: <username>, IP: <ipaddr>)	Informational
	Successful login through Web (SSL)	Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>)	Informational

Category	Event Description	Log Content	Severity
	Login failed through Web (SSL)	Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>)	Warning
	Logout through Web (SSL)	Logout through Web (SSL) (Username: <username>, IP: <ipaddr>)	Informational
	Web (SSL) session timed out	Web (SSL) session timed out (Username: <username>, IP: <ipaddr>)	Informational
Telnet	Successful login through Telnet	Successful login through Telnet (Username: <username>, IP: <ipaddr>)	Informational
	Login failed through Telnet	Login failed through Telnet (Username: <username>, IP: <ipaddr>)	Warning
	Logout through Telnet	Logout through Telnet (Username: <username>, IP: <ipaddr>)	Informational
	Telnet session timed out	Telnet session timed out (Username: <username>, IP: <ipaddr>)	Informational
SNMP	SNMP request received with invalid community string	SNMP request received from <ipAddress> with invalid community string!	Warning
STP	Topology changed	Topology changed (Instance:<InstanceID> port<portNum>)	Informational
	New Root selected	[CIST | CIST Regional | MSTI Regional] New Root bridge selected(Instance: <InstanceID> MAC: <macaddr> Priority :<value>)	Informational
	BPDU Loop Back on Port	BPDU Loop Back on Port <portNum>	Warning
	Spanning Tree Protocol is enabled	Spanning Tree Protocol is enabled	Informational
	Spanning Tree Protocol is disabled	Spanning Tree Protocol is disabled	Informational
	Root restriction enabled	Port <portNum> STP root restriction is enabled	Informational
	Root restriction disabled	Port <portNum> STP root restriction is disabled	Informational
SSH	Successful login through SSH	Successful login through SSH (Username: <username>, IP: <ipaddr>)	Informational
	Login failed through SSH	Login failed through SSH (Username: <username>, IP: <ipaddr>)	Warning
	Logout through SSH	Logout through SSH (Username: <username>, IP: <ipaddr>)	Informational
	SSH session timed out	SSH session timed out (Username: <username>, IP: <ipaddr>)	Informational
	SSH server is enabled	SSH server is enabled	Informational
	SSH server is disabled	SSH server is disabled	Informational
AAA	Authentication Policy is enabled	Authentication Policy is enabled (Module: AAA)	Informational
	Authentication Policy is disabled	Authentication Policy is disabled (Module: AAA)	Informational

Category	Event Description	Log Content	Severity
	Successful login through Console authenticated by AAA local method	Successful login through Console authenticated by AAA local method (Username: <username>)	Informational
	Login failed through Console authenticated by AAA local method	Login failed through Console authenticated by AAA local method (Username: <username>)	Warning
	Successful login through Web authenticated by AAA local method	Successful login through Web from <userIP> authenticated by AAA local method (Username: <username>)	Informational
	Login failed through Web authenticated by AAA local method	Login failed through Web from <userIP> authenticated by AAA local method (Username: <username>)	Warning
	Successful login through Web (SSL) authenticated by AAA local method	Successful login through Web (SSL) from <userIP> authenticated by AAA local method (Username: <username>)	Informational
	Login failed through Web (SSL) authenticated by AAA local method	Login failed through Web (SSL) from <userIP> authenticated by AAA local method (Username: <username>)	Warning
	Successful login through Telnet authenticated by AAA local method	Successful login through Telnet from <userIP> authenticated by AAA local method (Username: <username>)	Informational
	Login failed through Telnet authenticated by AAA local method	Login failed through Telnet from <userIP> authenticated by AAA local method (Username: <username>)	Warning
	Successful login through SSH authenticated by AAA local method	Successful login through SSH from <userIP> authenticated by AAA local method (Username: <username>)	Informational
	Login failed through SSH authenticated by AAA local method	Login failed through SSH from <userIP> authenticated by AAA local method (Username: <username>)	Warning
	Successful login through Console authenticated by AAA none method	Successful login through Console authenticated by AAA none method (Username: <username>)	Informational
	Successful login through Web authenticated by AAA none method	Successful login through Web from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful login through Web (SSL) authenticated by AAA none method	Successful login through Web (SSL) from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful login through Telnet authenticated by AAA none method	Successful login through Telnet from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful login through SSH authenticated by AAA none method	Successful login through SSH from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful login through Console authenticated by AAA server	Successful login through Console authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Login failed through Console authenticated by AAA server	Login failed through Console authenticated by AAA server <serverIP> (Username: <username>)	Warning

Category	Event Description	Log Content	Severity
	Login failed through Console due to AAA server timeout or improper configuration	Login failed through Console due to AAA server timeout or improper configuration (Username:<username>)	Warning
	Successful login through Web authenticated by AAA server	Successful login through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Login failed through Web authenticated by AAA server	Login failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Login failed through Web due to AAA server timeout or improper configuration	Login failed through Web from <userIP> due to AAA server timeout or improper configuration (Username:<username>)	Warning
	Successful login through Web (SSL) authenticated by AAA server	Successful login through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Login failed through Web (SSL) authenticated by AAA server	Login failed through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Login failed through Web(SSL) due to AAA server timeout or improper configuration	Login failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Successful login through Telnet authenticated by AAA server	Successful login through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Login failed through Telnet authenticated by AAA server	Login failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Login failed through Telnet due to AAA server timeout or improper configuration	Login failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Successful login through SSH authenticated by AAA server	Successful login through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Login failed through SSH authenticated by AAA server	Login failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Login failed through SSH due to AAA server timeout or improper configuration	Login failed through SSH from <userIP> due to AAA server timeout or improper Configuration (Username: <username>)	Warning
	Successful Enable Admin through Console authenticated by AAA local_enable method	Successful Enable Admin through Console authenticated by AAA local_enable method (Username: <username>)	Informational
	Enable Admin failed through Console authenticated by AAA local_enable method	Enable Admin failed through Console authenticated by AAA local_enable method (Username: <username>)	Warning
	Successful Enable Admin through Web authenticated by AAA local_enable method	Successful Enable Admin through Web from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational

Category	Event Description	Log Content	Severity
	Enable Admin failed through Web authenticated by AAA local_enable method	Enable Admin failed through Web from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning
	Successful Enable Admin through Web(SSL) authenticated by AAA local_enable method	Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational
	Enable Admin failed through Web(SSL) authenticated by AAA local_enable method	Enable Admin failed through Web(SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning
	Successful Enable Admin through Telnet authenticated by AAA local_enable method	Successful Enable Admin through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational
	Enable Admin failed through Telnet authenticated by AAA local_enable method	Enable Admin failed through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning
	Successful Enable Admin through SSH authenticated by AAA local_enable method	Successful Enable Admin through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational
	Enable Admin failed through SSH authenticated by AAA local_enable method	Enable Admin failed through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning
	Successful Enable Admin through Console authenticated by AAA none method	Successful Enable Admin through Console authenticated by AAA none method (Username: <username>)	Informational
	Successful Enable Admin through Web authenticated by AAA none method	Successful Enable Admin through Web from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful Enable Admin through Web (SSL) authenticated by AAA none method.	Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful Enable Admin through Telnet authenticated by AAA none method	Successful Enable Admin through Telnet from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful Enable Admin through SSH authenticated by AAA none method	Successful Enable Admin through SSH from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful Enable Admin through Console authenticated by AAA server	Successful Enable Admin through Console authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Enable Admin failed through Console authenticated by AAA server	Enable Admin failed through Console authenticated by AAA server <serverIP> (Username: <username>)	Warning

Category	Event Description	Log Content	Severity
	Enable Admin failed through Console due to AAA server timeout or improper configuration	Enable Admin failed through Console due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Successful Enable Admin through Web authenticated by AAA server	Successful Enable Admin through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Enable Admin failed through Web authenticated by AAA server	Enable Admin failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Enable Admin failed through Web due to AAA server timeout or improper configuration	Enable Admin failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Successful Enable Admin through Web(SSL) authenticated by AAA server	Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Enable Admin failed through Web (SSL) authenticated by AAA server	Enable Admin failed through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Enable Admin failed through Web(SSL) due to AAA server timeout or improper configuration	Enable Admin failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Successful Enable Admin through Telnet authenticated by AAA server	Successful Enable Admin through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Enable Admin failed through Telnet authenticated by AAA server	Enable Admin failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Enable Admin failed through Telnet due to AAA server timeout or improper configuration	Enable Admin failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Successful Enable Admin through SSH authenticated by AAA server	Successful Enable Admin through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Enable Admin failed through SSH authenticated by AAA server	Enable Admin failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Enable Admin failed through SSH due to AAA server timeout or improper configuration	Enable Admin failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	AAA server response is wrong	AAA server <serverIP> (Protocol: <protocolname>) response is wrong	Warning
	AAA doesn't support this functionality.	AAA doesn't support this functionality.	Informational

Category	Event Description	Log Content	Severity
	AAA server timed out	AAA server <serverIP> (Protocol: <protocol>) connection failed	Warning
Port security	Port security has exceeded its maximum learning size and will not learn any new addresses	Port security violation (Port: <portNum>, MAC: <macaddr>)	Warning
	Port security write one permanent record to flash	<portNum> port security entry (Port: <portNum>, index: <index>, VID: <vlanid>, MAC: <macaddr>)	Informational
IP and Password Changed	IP Address change activity	Management IP address was changed into <ipAddr> by (Username: <username>, IP:<ipaddr>)	Informational
	IP Address change activity by console	Management IP address was changed into <ipAddr> by console (Username: <username>)	Informational
	Password change activity	User <username> Password was changed by (Username: <username>, IP:<ipaddr>)	Informational
	Password change activity by console	User <username> Password was changed by console (Username: <username>)	Informational
Packet Storm	Broadcast strom occurrence	Port <portNum> Broadcast storm is occurring	Warning
	Broadcast storm cleared	Port <portNum> Broadcast storm has cleared	Informational
	Multicast storm occurrence	Port <portNum> Multicast storm is occurring	Warning
	Multicast storm cleared	Port <portNum> Multicast storm has cleared	Informational
	Port shutdown due to a packet storm	Port <portNum> is currently shutdown due to a packet storm	Warning
	Configuration Testing Protocol detects a loop in port	Configuration Testing Protocol detects a loop in port <portNum>	Informational
802.1x	VID assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully .This VID will be assigned to the port and this port will be the VLAN untagged port member.	Radius server <ipaddr> assigned VID: <vlanid> to Port <portNum> (Account: <username>)	Informational
	802.1x Authentication failure	802.1x Authentication failure from (Username: <username>, Port <portNum>, MAC: <macaddr>)	Warning
	802.1x Authentication failure for the radius server timeout	802.1x Authentication failure for the radius server <ipaddr> timeout from (Username: <username>, Port <portNum>, MAC: <macaddr>)	Warning
	802.1x Authentication failure for the 802.1X client session timeout	802.1x Authentication failure for the 802.1X client session timeout from (Username: <username>, Port <portNum>, MAC: <macaddr>)	Warning
	802.1x Authentication success	802.1x Authentication success from (Username: <username>, Port <portNum>, MAC: <macaddr>)	Informational

Category	Event Description	Log Content	Severity
MAC-based Access Control	MAC-based Access Control host login successful	MAC-based Access Control host login successful (MAC: <macaddr>, port: <portNum>, VID: <vlanid>)	Informational
	MAC-based Access Control unauthenticated host	MAC-based Access Control unauthenticated host(MAC: <macaddr>, Port: <portNum>, VID: <vlanid>)	Critical
	MAC-based Access Control host aged out	MAC-based Access Control host aged out (MAC: <macaddr>, port: <portNum>, VID: <vlanid>)	Informational
Loopback Detection	Port recovers from Loopback Detection err-disabled state manually.	Port <portNum> recovers from Loopback Detection err-disabled state manually.	Informational
	Port recovers from Loopback Detection err-disabled state automatically.	Port <portNum> recovers from Loopback Detection err-disabled state automatically.	Informational

APPENDIX B

Trap List

Trap Name/OID	Variable Bind	Format	Description	MIB Name
coldStart 1.3.6.1.6.3.1.1.5.1	None	V2	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.	RFC1907 (SNMPv2-MIB)
warmStart 1.3.6.1.6.3.1.1.5.2	None	V2	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.	RFC1907 (SNMPv2-MIB)
authenticationFailure 1.3.6.1.6.3.1.1.5.5	None	V2	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.	RFC1907 (SNMPv2-MIB)
linkDown 1.3.6.1.6.3.1.1.5.3	ifIndex, ifAdminStatus, ifOperStatus	V2	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.	RFC2863 (IF-MIB)

Trap Name/OID	Variable Bind	Format	Description	MIB Name
linkUp 1.3.6.1.6.3.1.1.5.4	ifIndex, ifAdminStatus, ifOperStatus	V2	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.	RFC2863 (IF-MIB)
newRoot 1.3.6.1.2.1.17.0.1	None	V2	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election. Implementation of this trap is optional.	RFC1493 (BRIDGE-MIB)
topologyChange 1.3.6.1.2.1.17.0.2	None	V2	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.	RFC1493 (BRIDGE-MIB)
risingAlarm 1.3.6.1.2.1.16.0.1	alarmIndex, alarmVariable, alarmSampleType, alarmValue, alarmRisingThreshold	V2	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.	RFC2819 (RMON-MIB)
fallingAlarm 1.3.6.1.2.1.16.0.2	alarmIndex, alarmVariable, alarmSampleType, alarmValue, alarmFallingThreshold	V2	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.	RFC2819 (RMON-MIB)

Trap Name/OID	Variable Bind	Format	Description	MIB Name
lldpRemTablesChange 1.0.8802.1.1.2.0.0.1	lldpStatsRemTablesInserts, lldpStatsRemTablesDeletes, lldpStatsRemTablesDrops, lldpStatsRemTablesAgeouts	V2	A lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes. It can be utilized by an NMS to trigger LLDP remote systems table maintenance polls.	LLDP (LLDP-MIB)